EXTRAHOP

ExtraHop RevealX™ for Kubernetes

Real-time network intelligence that reveals what's actually happening in your dynamic K8s infrastructure

SOLUTION BRIEF

The Challenge

Kubernetes (K8s) has evolved from a container orchestrator into the control plane for modern infrastructure—supporting cloud-native applications and increasingly autonomous, AI-driven systems. It delivers an enormous amount of flexibility for automating, scaling, and maintaining complex systems without manual intervention. But with that power comes complexity and risk.

Operational Blind Spots

- Traditional monitoring tools built for static environments can't keep pace with Kubernetes' ephemeral, constantly changing infrastructure
- Metrics, logs, and traces provide fragmented views that leave critical gaps in understanding actual system behavior
- Kubernetes abstracts away infrastructure and operational details so humans don't have to reason about individual machines in a large-scale environment, but this abstraction makes root cause analysis time-consuming and difficult

Expanding Attack Surface

- Kubernetes requires specialized knowledge to manage effectively and can easily be misconfigured, exposing your organization to cryptomining, data exfiltration, and lateral movement
- Container runtimes and software supply chains create new vulnerability vectors that adversaries actively exploit
- Kernel-level container escapes can compromise entire nodes and grant attackers access to sensitive data across multiple workloads
- Encrypted service mesh traffic sharply limits visibility, rendering most network-based inspection approaches ineffective

The Cost of Complexity

- Mean Time to Remediate (MTTR) increases as teams struggle to correlate data across siloed tools
- Mean Time to Contain (MTTC) grows while security teams hunt for threats without complete visibility
- Elastic scaling, while powerful, can drive unexpected cost overruns without proper monitoring

KEY CAPABILITIES

Reveal a more complete picture of actual behavior in a dynamic cluster and across hybrid environments

See the root cause of latency—the platform, the application, or the network

Uncover threats hiding in encrypted and unencrypted traffic

Preserve a history of record for future investigation, auditing, and compliance

How ExtraHop Solves the Challenge

Correlating K8s Ephemeral Data with Network Ground Truth

RevealX observes every connection, dependency, and performance signal at the network level—giving your teams definitive answers when incidents occur.

For IT Operations Leaders

Accelerate Incident Resolution

- Pinpoint whether performance issues stem from the platform, application, or network layer—eliminating hours of troubleshooting
- Monitor latency and resource efficiency across ephemeral workloads in real time
- Reduce MTTR by quickly identifying the root cause of service degradation, retry storms, or congestion

Control Costs While Maintaining Reliability

- Gain visibility into east-west traffic patterns that drive unexpected resource consumption
- Identify inefficient service interactions before they impact SLAs or budgets
- Ensure AI models and critical applications maintain responsiveness under varying load conditions

For Security Operations Leaders

Detect Threats in Encrypted Environments

- Identify anomalous behavior in east-west traffic
- Establish baselines for normal service-to-service communication and alert on deviations
- Detect when containers communicate with unexpected destinations—a key indicator of compromise

Contain Threats Faster

- Correlate Kubernetes metadata (namespace, pod, replica set) with network behavior automatically
- Leverage integrated threat intelligence to detect communication with known C2 infrastructure
- Reduce MTTC by eliminating manual correlation across data silos

Maintain an Immutable Audit Trail

- Preserve a complete network record for forensic analysis and compliance
- Validate that security controls are functioning as intended
- Ensure adversaries haven’t bypassed or corrupted your security logic

How It Works

Network-Level Ground Truth

Logs and metrics are emitted by applications, runtimes, and K8s components that understand the desired state. They reflect the system's internal view—what the platform believes should be happening. ExtraHop observes what actually *is* happening on the wire. Every packet, every connection, every transaction becomes high-fidelity intelligence about real application behavior that is independent of configuration, instrumentation, or intent.

Automated Correlation at Scale

RevealX automatically enriches network data with Kubernetes context by linking IP addresses to ephemeral pods, namespaces, and services. This eliminates the manual work of stitching together disparate data sources during incidents.

Behavioral Analysis for Dynamic Environments

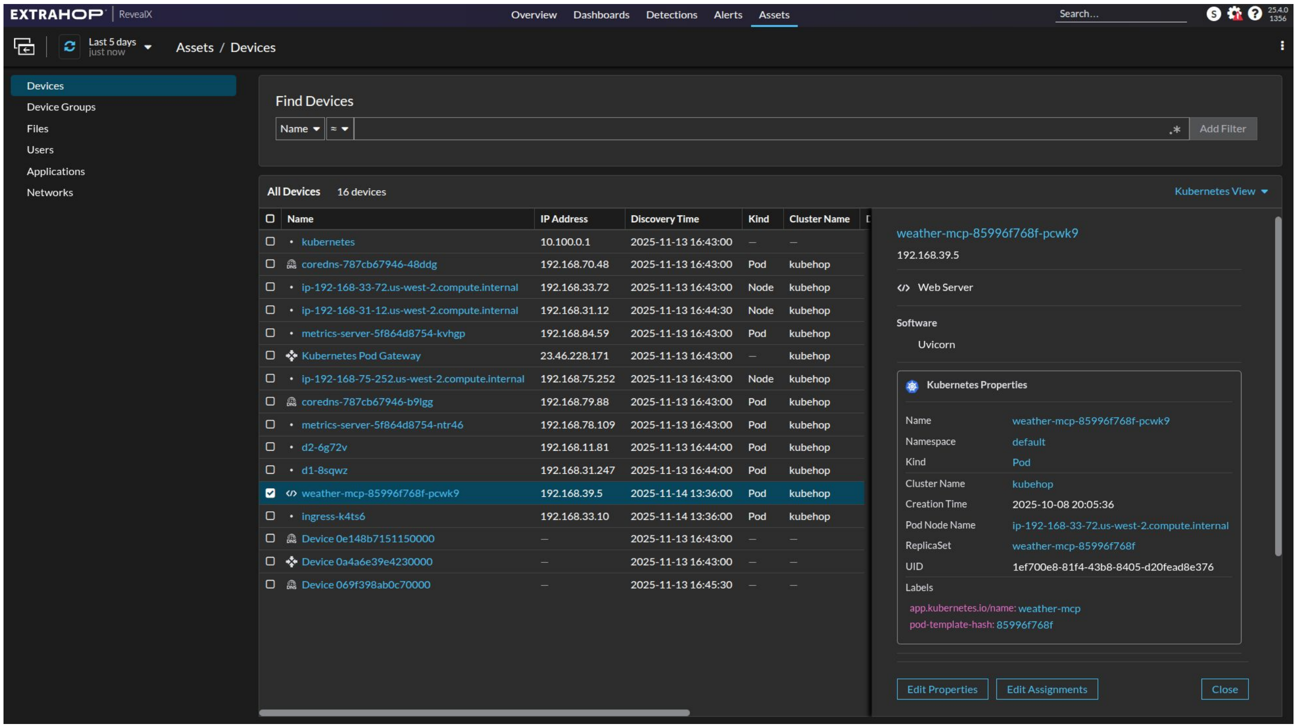
In Kubernetes, east-west traffic is constant. The question isn't "is there traffic?"—it's "is this normal for this service?" RevealX baselines behavior patterns and alerts when workloads exhibit anomalous activity, such as:

- A container suddenly communicating with services it has never contacted before
- Unusual data transfer volumes between pods
- Access patterns inconsistent with normal application behavior

Enriched Context for Decisive Action

RevealX correlates network telemetry with:

- **Identity data** to detect credential misuse or privilege escalation
- **Threat intelligence** to identify communication with malicious infrastructure
- **Kubernetes metadata** to understand the blast radius of potential compromises



All Devices 16 devices

☐	Name	IP Address	Discovery Time	Kind	Cluster Name
☐	kubernetes	10.100.0.1	2025-11-13 16:43:00	—	—
☐	coredns-787cb67946-48ddg	192.168.70.48	2025-11-13 16:43:00	Pod	kubehop
☐	ip-192-168-33-72.us-west-2.compute.internal	192.168.33.72	2025-11-13 16:43:00	Node	kubehop
☐	ip-192-168-31-12.us-west-2.compute.internal	192.168.31.12	2025-11-13 16:44:30	Node	kubehop
☐	metrics-server-5f864d8754-kvhgp	192.168.84.59	2025-11-13 16:43:00	Pod	kubehop
☐	Kubernetes Pod Gateway	23.46.228.171	2025-11-13 16:43:00	—	kubehop
☐	ip-192-168-75-252.us-west-2.compute.internal	192.168.75.252	2025-11-13 16:43:00	Node	kubehop
☐	coredns-787cb67946-b9lgg	192.168.79.88	2025-11-13 16:43:00	Pod	kubehop
☐	metrics-server-5f864d8754-ntr46	192.168.78.109	2025-11-13 16:43:00	Pod	kubehop
☐	d2-6g72v	192.168.11.81	2025-11-13 16:44:00	Pod	kubehop
☐	d1-8sqwz	192.168.31.247	2025-11-13 16:44:00	Pod	kubehop
☑	weather-mcp-85996f768f-pcwk9	192.168.39.5	2025-11-14 13:36:00	Pod	kubehop
☐	ingress-k4ts6	192.168.33.10	2025-11-14 13:36:00	Pod	kubehop
☐	Device 0e148b7151150000	—	2025-11-13 16:43:00	—	—
☐	Device 0a4a6e39e4230000	—	2025-11-13 16:43:00	—	—
☐	Device 069f398ab0c70000	—	2025-11-13 16:45:30	—	—

weather-mcp-85996f768f-pcwk9
192.168.39.5

Web Server

Software
Uvicorn

Kubernetes Properties

Name	weather-mcp-85996f768f-pcwk9
Namespace	default
Kind	Pod
Cluster Name	kubehop
Creation Time	2025-10-08 20:05:36
Pod Node Name	ip-192-168-33-72.us-west-2.compute.internal
ReplicaSet	weather-mcp-85996f768f
UID	1ef700e8-81f4-43b8-8405-d20fead8e376

Labels
app.kubernetes.io/name: weather-mcp
pod-template-hash: 85996f768f

Figure 1: Select a pod or node to see Kubernetes properties. Filter by namespace, cluster, deployment, ReplicaSet, and more.

Business Outcomes

Reclaim Hundreds of Hours Annually

Eliminate manual correlation work during incidents. Your teams get immediate context instead of hunting across multiple tools.

Improve Security Posture

Detect lateral movement and data exfiltration attempts that bypass traditional perimeter defenses and evade endpoint detection.

Accelerate Digital Initiatives

Deploy confidently in Kubernetes environments knowing you have comprehensive visibility into performance and security.

Support AI-Driven Operations

Clean, high-fidelity network data ensures AI agents and automation platforms can make accurate decisions at machine speed—eliminating the “garbage in, garbage out” problem that plagues traditional telemetry.

Ensure Operational Resilience

Maintain an immutable record of network activity that supports compliance requirements and provides the audit trail needed for post-incident analysis.

Why ExtraHop

While metrics, logs, and traces are necessary components of observability, they provide incomplete pictures of dynamic Kubernetes environments. ExtraHop RevealX delivers the network-level ground truth that ties everything together—revealing what's actually happening across your hybrid infrastructure, not just what Kubernetes reports should be happening.

For security and IT operations leaders managing the complexity and risk of containerized environments, RevealX provides the definitive source of truth needed to operate confidently at scale.

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk. Learn more at extrahop.com.

EXTRAHOP®

info@extrahop.com
extrahop.com