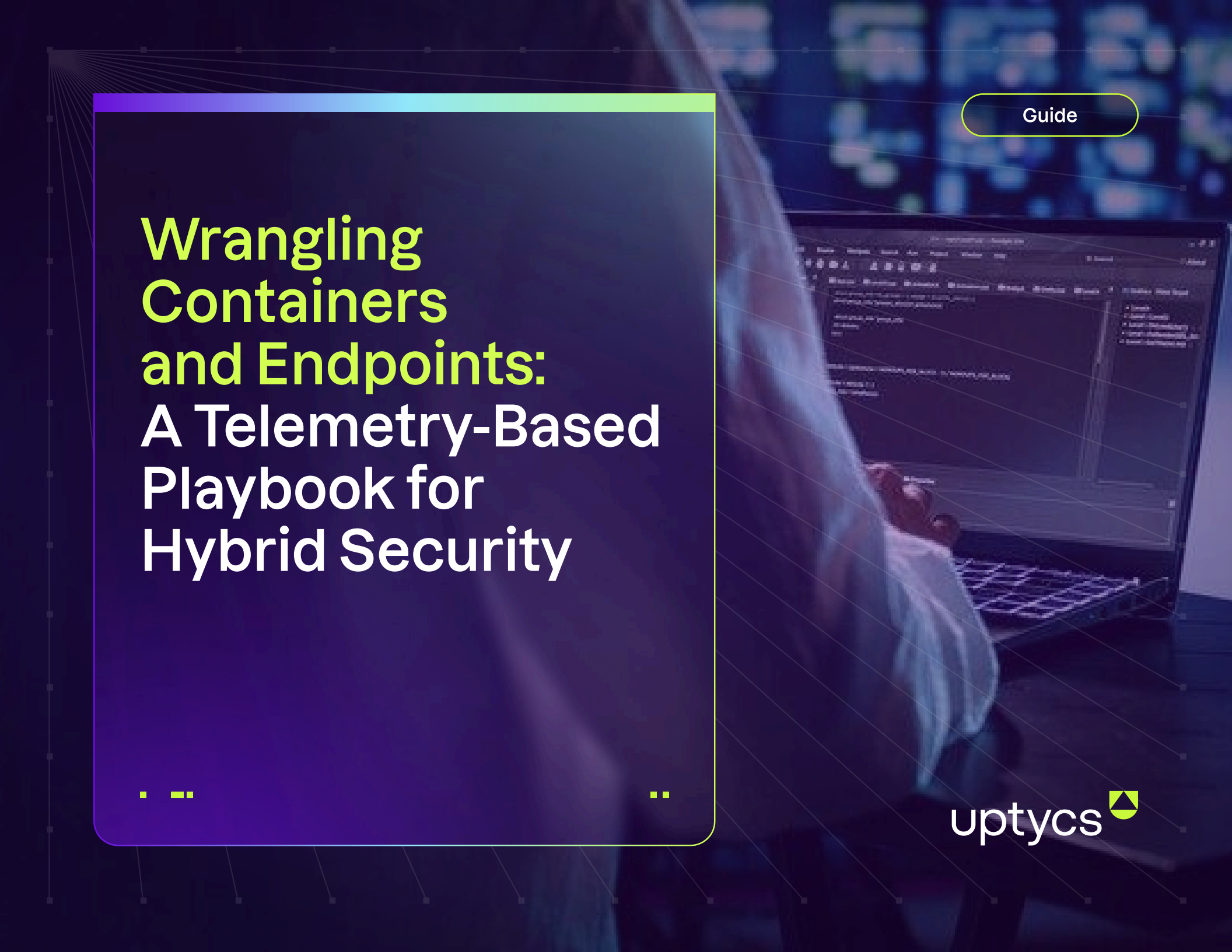
Guide

Wrangling Containers and Endpoints: A Telemetry-Based Playbook for Hybrid Security



uptycs

Table of Contents

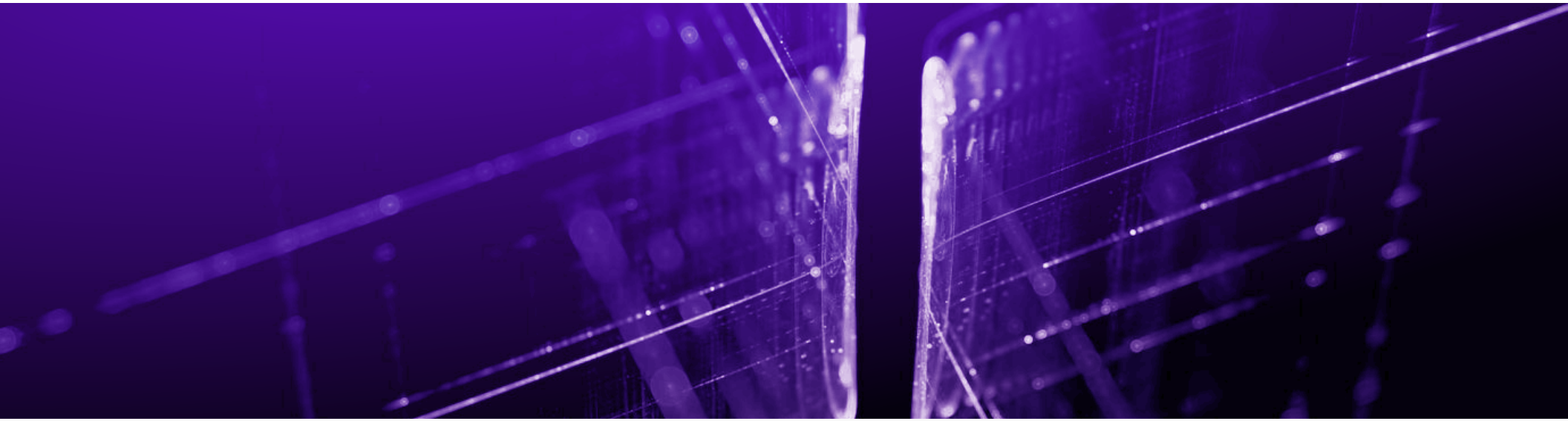
Why Hybrid Security Demands a New Playbook

The answer lies in telemetry.

Modern organizations are running in two worlds at once. On one side, containerized workloads and Kubernetes orchestration drive innovation at speed and scale. On the other, diverse endpoints from corporate laptops to remote devices remain the everyday tools of productivity, and therefore prime targets for attackers.

The challenge is clear: hybrid environments combine the complexity of ephemeral container clusters with the persistence and variability of endpoints. Security teams often end up with fragmented visibility and siloed tooling, leaving critical blind spots when threats move across these domains.

The answer lies in telemetry. By collecting and unifying detailed, normalized signals across both containers and endpoints, telemetry creates a shared foundation for detection, response, and governance. This playbook offers practical steps to simplify hybrid security through telemetry, bridging the gaps between control planes and endpoints.



Understanding the Complexity of Containers and Endpoints

Hybrid security requires a unified approach, one that starts with visibility across the full environment.

Kubernetes Complexity

Kubernetes has become the de facto standard for orchestrating containerized workloads, but its scale and dynamism create new challenges. Containers are ephemeral by nature, spinning up and down in seconds. Multiple clusters and control planes make governance difficult, while shared responsibility models often blur the lines between infrastructure and application security.

Endpoint Challenges

Endpoints remain a major attack surface. They come in many forms: Windows laptops, Linux servers, developer workstations, and bring-your-own devices. Remote work has expanded this surface area further, creating environments that are diverse, loosely managed, and vulnerable to persistence techniques that attackers exploit.

The Hybrid Dilemma

When an incident spans both domains, for example an attacker moves from a compromised endpoint into a containerized application, teams often struggle to piece together the full picture. Tooling and teams are frequently siloed, leading to delays in detection and inconsistent response.

Hybrid security requires a unified approach, one that starts with visibility across the full environment.

Field Note:
When assessing your hybrid environment, map not only the assets you know but also those that are ephemeral or transient. Blind spots often emerge in the spaces between traditional endpoints and rapidly changing container workloads.

Telemetry for Complete Visibility

Logs are often siloed and inconsistent, requiring heavy manual parsing before they can provide actionable insights.

Defining Telemetry in Hybrid Security

Telemetry refers to the continuous collection of data points from systems, applications, and workloads. In a hybrid environment, this means gathering signals from Kubernetes clusters, containers, endpoints, and cloud services. Unlike raw logs, telemetry is structured and normalized, making it easier to correlate events across diverse systems.

Why Raw Logs Aren't Enough

Logs are often siloed and inconsistent, requiring heavy manual parsing before they can provide actionable insights. Telemetry streamlines this by presenting security-relevant data in a unified format, reducing noise and improving time to detection.

Bridging Perspectives

Telemetry acts as a shared language between DevOps, IT, and security teams. Developers can see how workloads behave in production, operators can monitor performance and policy adherence, and security teams can detect malicious patterns, all from the same dataset.

Field Note:
To build a telemetry pipeline that scales, start by mapping sources across both containers and endpoints. Normalize signals for consistency, centralize collection into a unified platform, and enrich data with metadata like user, device, or container image for context.

Industry Note: Independent analysis from the EDR Telemetry Project highlights leaders in Linux EDR telemetry, underscoring the value of deep and consistent telemetry for hybrid defense.

EDR and Kubernetes: A Unified Threat Response Approach

With telemetry, the events can be correlated: endpoint compromise, credential misuse, and container intrusion become part of a single attack narrative, enabling faster and more effective response.

Why the Gap Exists

Traditional Endpoint Detection and Response was designed for persistent devices like laptops and servers. Containers, by contrast, are ephemeral and orchestrated by Kubernetes. Traditional EDR cannot keep pace with their rapid lifecycle.

Leveraging Telemetry for Cross-Domain Threats

Telemetry closes the gap by normalizing signals across both domains. A single stream of enriched data allows detection rules and response playbooks to apply consistently, regardless of whether the threat originates on an endpoint or inside a container.

Case-in-Action: Stopping Lateral Movement

Imagine an attacker compromises a developer laptop, steals credentials, and uses them to pivot into a Kubernetes cluster. Without unified telemetry, security teams may treat these as separate incidents. With telemetry, the events can be correlated: endpoint compromise, credential misuse, and container intrusion become part of a single attack narrative, enabling faster and more effective response.

Field Note:
Align SOC and DevOps teams around shared telemetry dashboards. Define unified detection rules that apply across environments, and automate containment workflows that can act across both clusters and devices.

Simplifying Compliance Across Containers and Endpoints

> **By continuously collecting normalized data, telemetry provides an always-on evidence trail.**

The Compliance Challenge

Organizations face a growing list of frameworks such as CIS Benchmarks, PCI-DSS, HIPAA, and SOC 2. Each requires evidence of secure configuration and continuous monitoring. In hybrid environments, compliance complexity multiplies.

- Containers: Ephemeral nodes complicate continuous evidence collection
- Endpoints: Diversity of devices makes standardization difficult
- Teams: Responsibility is often split across security, DevOps, and compliance groups

Telemetry as Evidence

By continuously collecting normalized data, telemetry provides an always-on evidence trail. Instead of scrambling for audit reports at year-end, organizations can demonstrate compliance on demand.

Field Note:
Map telemetry fields directly to compliance controls, automate reporting, and benchmark configurations against standards like CIS for Kubernetes and Linux. This shifts compliance from an audit-time scramble to continuous readiness.

From Control Planes to Endpoints: Unified Governance with Telemetry

> **Telemetry doesn't just improve visibility, it enables governance.**

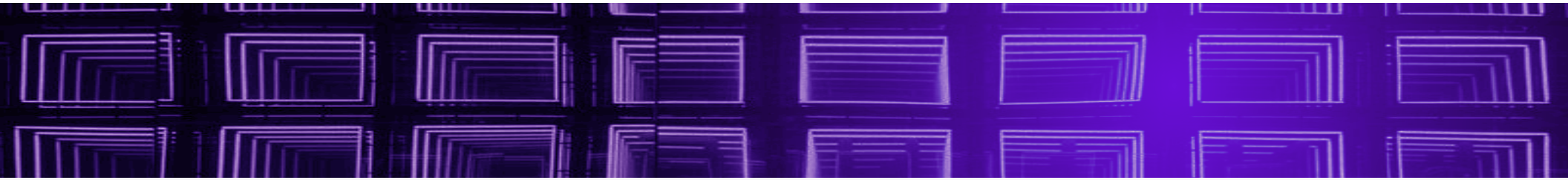
Beyond Visibility: Governance at Scale

Telemetry doesn't just improve visibility, it enables governance. By applying consistent rules and policies across environments, organizations can reduce risk and improve operational efficiency.

Step-by-Step Governance with Telemetry

1. **Map Telemetry Sources:** Identify all endpoints, clusters, and services
2. **Normalize and Enrich Data:** Ensure consistent structure and add context
3. **Apply Controls:** Enforce security baselines across workloads and devices
4. **Automate Detection and Response:** Set automated alerts and playbooks for policy violations
5. **Continuously Refine:** Use telemetry insights to adapt policies as environments evolve

Field Note:
Operationalize governance by making telemetry the backbone of both security controls and compliance. This ensures consistency across clusters, endpoints, and the teams that manage them.



Telemetry in Action: The Uptycs Advantage

The EDR Telemetry Project ranks Uptycs number one for Linux EDR telemetry visibility as of May 2025.

The challenges of hybrid security, including ephemeral containers, diverse endpoints, and complex compliance, demand a telemetry-first approach.

Uptycs delivers this through a unified platform that combines CNAPP capabilities with market-leading EDR. The EDR Telemetry Project ranks Uptycs number one for Linux EDR telemetry visibility as of May 2025, reflecting its ability to provide unmatched coverage across containerized and endpoint environments.

By integrating container and endpoint telemetry into a single plane of visibility, Uptycs enables faster detection, streamlined compliance, and more consistent governance. For organizations navigating hybrid complexity, this unified approach turns telemetry into a competitive advantage.

Industry Note: Recognition as number one in Linux EDR telemetry visibility highlights the role of deep telemetry in shaping the next generation of hybrid defense.

uptycs

Uptycs is dedicated to leading security innovations in hybrid cloud environments, ensuring robust protection and enabling our customers to innovate safely and efficiently. Included in the 2024 CNAPP Market Guide, Uptycs provides comprehensive security solutions that bridge the gap from code to cloud. Our platform excels in Cloud Workload Protection (CWPP), Vulnerability Management, Cloud Security Posture Management (CSPM), Detection & Response, Software Pipeline Security, XDR, and Risk & Compliance. Trusted by leading enterprises like PayPal and Comcast, Uptycs transforms potential vulnerabilities into fortified security, ensuring your digital environments are safeguarded from development through runtime.

Secure Everything from Dev to Runtime

Learn more at Uptycs.com