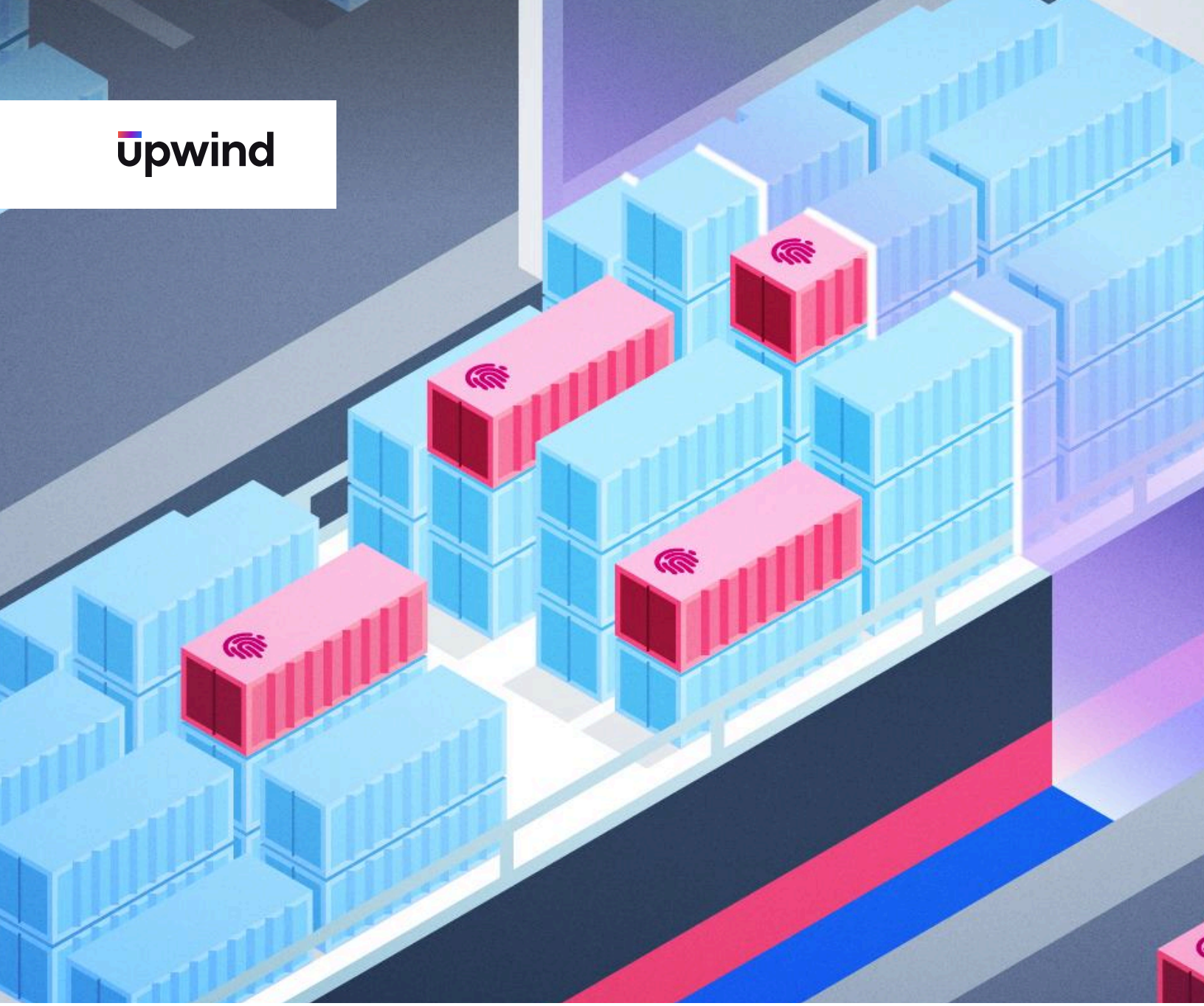
upwind



BEST PRACTICES

API Security: The Unseen Risk in Your Cloud Environment

API Security

APIs are the backbone of modern applications—connecting services, moving data, and enabling automation across cloud environments. But while they drive innovation, they're often left out of the core security conversation.

Traditional tools don't provide the context needed to secure APIs effectively. They surface issues but fail to explain what's actually at risk. Without real-time insight, API threats go undetected—until it's too late.

That's where **Upwind** comes in.

The Hidden Dangers of API Security Gaps

APIs are a common attack vector—and for good reason.

Traditional security stacks weren't built for the dynamic, ephemeral nature of API traffic in the cloud. The risks? Often invisible until it's too late.

Here's what static tools miss:

- **Exposed endpoints leaking sensitive data**—without anyone knowing.
- **Misconfigured APIs accepting unvalidated inputs—**leading to injection, abuse, or full-blown breaches.
- **Lack of traceability across distributed services—**making it nearly impossible to follow the flow of requests and responses in real time.

The attack surface keeps growing.

Your visibility? Not so much.

How Upwind Protects APIs with Runtime Context

Upwind doesn't just scan APIs. It *understands* them.

By analyzing live traffic and behavior across your cloud, Upwind delivers API security that's intelligent, automated, and deeply contextual.

Discovers and classifies APIs in real time

- Finds exposed, unauthenticated, and high-risk APIs as they emerge
- Highlights shadow APIs that static inventories miss

Maps API calls across services and environments

- Detects abnormal flows, suspicious communication patterns, and sensitive data risks
- Connects API activity to users, workloads, and infrastructure

Monitors for abuse without adding friction

- Flags anomalies and potential threats before they escalate
- Prioritizes issues based on real risk—not theoretical vulnerabilities

Real-World Impact: Solving API Security at Cloud Speed

One Upwind customer used our runtime API protection to:

- Prevent unauthorized sensitive data flows
- Automatically detect and flag OWASP Top 10 API vulnerabilities
- Detect API threats production in real time

Read the full case study →

The Future of API Security is Continuous and Context-Aware

You can't protect what you can't see.

APIs are dynamic, distributed, and critical to your business. They deserve more than periodic scans and retroactive alerts.

Upwind provides you:

- Dynamic API discovery and cataloging
- Real-time threat detection
- Intelligent vulnerability testing and risk prioritization
- Seamless integration into existing workflows

Upwind doesn't just show you the risk—it gives you the power to eliminate it, in real time.

Get a demo at upwind.io →