



CUSTOMER SNAPSHOT

PepsiCo

Cyber Fusion Center

Two engineers, one platform, zero attribution: How PepsiCo's Cyber Fusion Center consolidated its riskiest work on Kasm Workspaces.

PepsiCo's 24x7x365 Cyber Fusion Center replaced a commercial isolation service and analyst "dirty laptops" with self-hosted Kasm Workspaces — consolidating incident response, threat intelligence and malware analysis on one non-attributable platform, built and run by a two-person team that now ships its own workspaces when the catalog doesn't have what it needs.



<24 hrs

from analyst problem to a new capability
built, tested and deployed



Zero

research traffic attributable to PepsiCo —
isolated lab, managed egress



4 → 1

research use cases consolidated on one
platform



2 engineers

built, scaled and run the whole self-hosted
deployment



INDUSTRY

Food, beverage &
agriculture



SCALE

Fortune 50, global,
24x7x365



DEPLOYMENT

Self-hosted, multi-
server



REPLACED

Silo (Authentic8),
laptops, homelabs



The challenge

Before Kasm, the team ran a patchwork: Silo (Authentic8) for isolated browsing plus individually issued secondary laptops and analyst homelabs for everything else — an arrangement the team describes as “not sustainable or good in any sense.”

Two things forced a change: a substantial price increase, and failures on work the team cannot compromise on.

- ✓ No control over the platform; little open documentation
- ✓ Repeated failures on the large downloads dark web casework requires
- ✓ Could not meet PepsiCo's six-year evidence retention policy
- ✓ DNS and traceability leaks while detonating samples — met with a “renew first, then we'll troubleshoot” response

For a lab whose first principle is **non-attribution**, a traceability leak is not a bug it is a threat to the mission.



The Kasm solution

The Cyber Fusion Center runs a self-hosted Kasm Workspaces deployment on its own isolated lab infrastructure. Every session is a disposable, containerized browser or full desktop: phishing sites, dark web research and live malware execution never touch an analyst endpoint or the corporate network.

Workspace per job

Default Kasm browsers and the official Tor workspace; in-house VPN- and Tor-enabled “SquirrelWorks” workspaces for IR and CTI; a custom REMnux workspace for malware analysis.

Egress built for non-attribution

Kasm's PureVPN integration keeps investigative traffic off PepsiCo IP space. “Tremendously” important, the team says — “a must.”

A real build pipeline

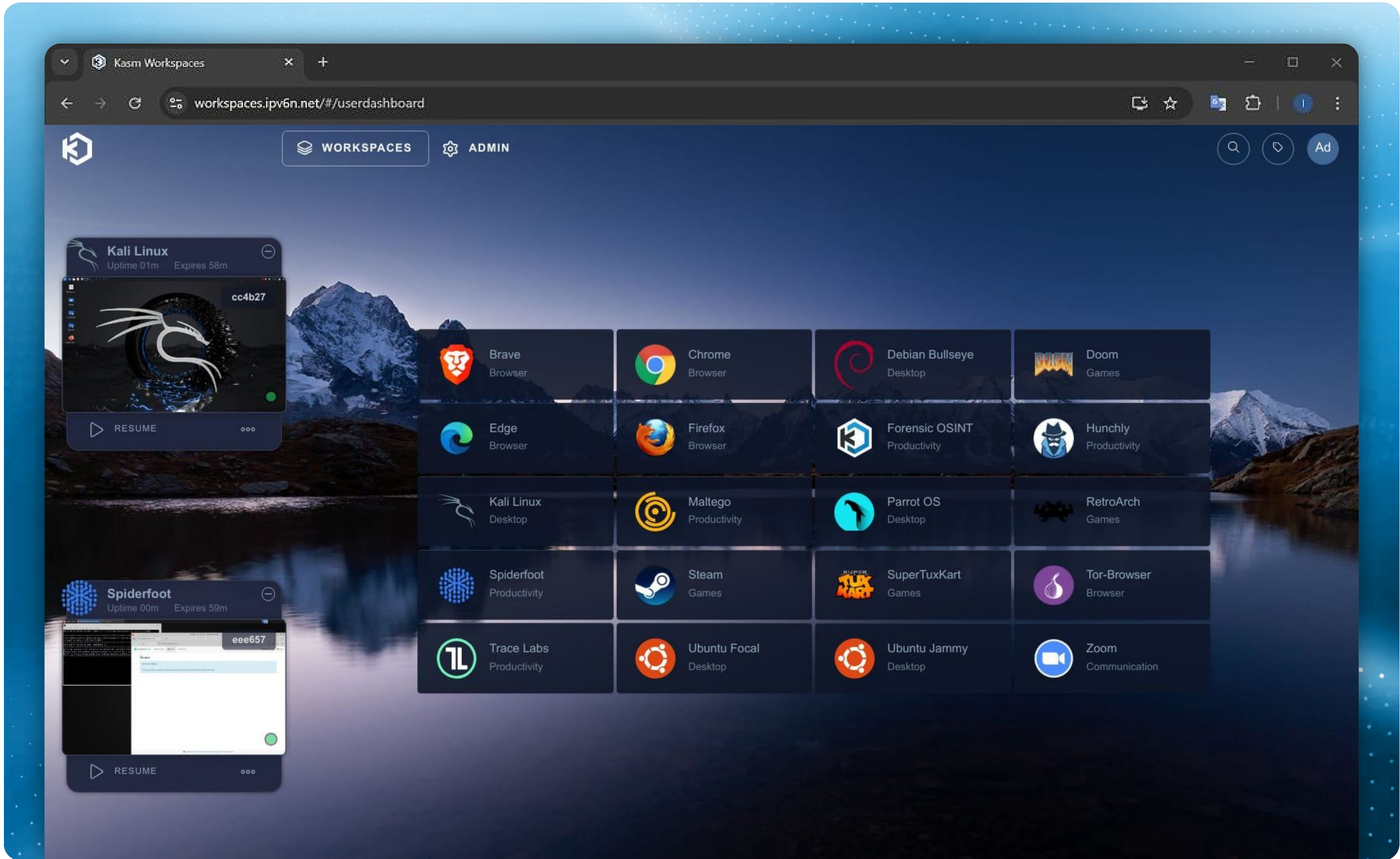
Lint, build, scan the core image, publish to a registry, auto-pull into Kasm. Every custom capability is reproducible and version-controlled.

Why PepsiCo chose Kasm

The team evaluated standard virtualization and per-analyst dirty machines; nothing met the full requirement set. Kasm did — but the deciding factor was not the feature list. Open documentation and an active community meant a two-person engineering team could build around any gap itself, including entirely new workspaces. And when the pair were about to buy their own egress solution, Kasm announced PureVPN integration; they scrapped the plan and bought licenses instead.

“It wasn't about how flexible Kasm was to meet our needs — it was how flexible it could be.”

- James Konderla,
Threat Response Management Associate Principal, PepsiCo



From Problem to Shipped Capability in 24 Hours

Shortly after the move, the threat intelligence team tested its new dark web capability by pulling a large file tied to an active case. The download kept failing — the threat actor's infrastructure kept going up and down. Under the old model that meant a support ticket and a wait. Instead, PepsiCo's engineer modified the custom SquirrelWorks workspace, tested it and deployed it within 24 hours. Analysts can now stop, pause and resume interrupted downloads over Tor inside the workspace. The team has since re-deployed to a multi-server architecture on its own and plans to add multi-zone once its AWS environment is provisioned.

Results

Metric	Before	with  Kasm WORKSPACES	Impact
 Time to deliver a new analyst capability	Dependent on vendor roadmap and renewal	Modified, tested and deployed in-house	<24 hours
 Research traffic attributable to PepsiCo	DNS and traceability leaks observed during sample execution	Isolated lab, managed VPN and Tor egress	Zero
 Research platforms in use	Isolation service + laptops + homelabs	One self-hosted Kasm deployment	4 use cases → 1
 Platform engineering team	Vendor-dependent for fixes and changes	Self-built multi-server deployment, in-house workspaces	2 engineers
 Six-year evidence retention	Not supported by prior platform	Retained under the lab's own control	Requirement met

“When we first adopted Kasm we wanted a solution to replace a competitor's problem. Since then we now develop our own workspaces to meet our specific use cases, host our own isolated solution and eagerly follow Kasm's patch and development notes to integrate them as a key feature in our lab's use cases.”

- James Konderla, Threat Response Management Associate Principal, PepsiCo

