



Run Your Infrastructure *with Confidence*

Our Hardened Runtime stops attacks before your detection tool fires an alert.
95% less attack surface. 100% more confidence.

Overview

Stop chasing bad alerts. Our hardened runtime cuts attack surfaces by 95%, preventing breaches and enabling secure multi-tenancy at scale. While other solutions force tradeoffs between security, performance & resource efficiency, we deliver all three simultaneously. Organizations ship with containers but transform with Edera, achieving significant infrastructure cost savings and security by default.

Products



Edera For Containers

Our hardened runtime reduces attack surface and enables secure multi-tenancy at scale. Provision tenant environments declaratively with complete control over isolation, performance, and cost.



Edera For AI Agents

Accelerate AI innovation with optimized resource utilization. Our enhanced GPU virtualization technology lets you safely share expensive GPU resources across multiple workloads, reducing cloud costs while maintaining full performance and isolation.



Edera for GPUs

Scaling GPU accessibility through true isolation. Edera's platform safely slices GPU resources across workloads, enabling multiple applications to securely share infrastructure.

Why Edera

Minimal

Edera cuts your attack surface by 95%. Built on the Xen hypervisor, our minimal platform strips away the bloat – less code, fewer vulnerabilities, stronger security.

Secure

Edera's hardened runtime brings security closer to the hardware, enforces trust by design, makes observability actionable, and secures multi-tenant workloads.

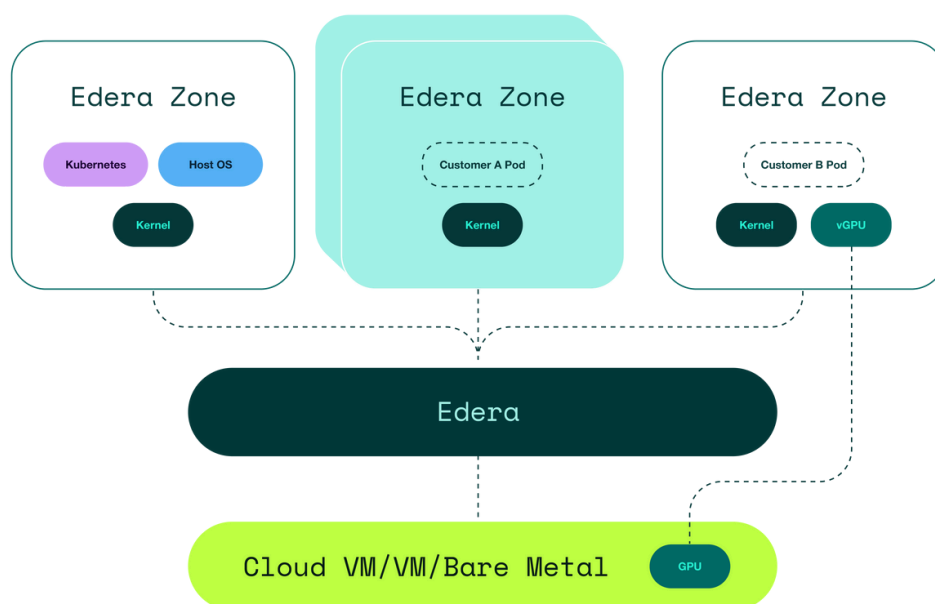
Fast

Our platform delivers performance within 5% of native containers and requires no specialized hardware or changes to existing development workflow.



See Edera in Action

Proactive runtime security that delivers true isolation and secure multi-tenancy across your workloads



Edera for Containers		Edera for GPUs	
Container Isolation	✓	Driver Isolation and Secure vGPUs	✓
Eliminates Shared Kernel and Container Runtime Vulnerabilities	✓	Simplified GPU Device Virtualization	✓
FIPS Kernel Support	✓	Supports All Hardware Accelerators: GPUs, TPUs, and DPUs	✓
Native Performance	✓	Driving the Industry Forward with Virtual Device Functions in GPUs	✓
Autoscale and Dynamic Workload Resources	✓	Support for Confidential Computing	✓
Live Container Migration and Memory Ballooning	✓	Production-Grade Sandboxing	✓