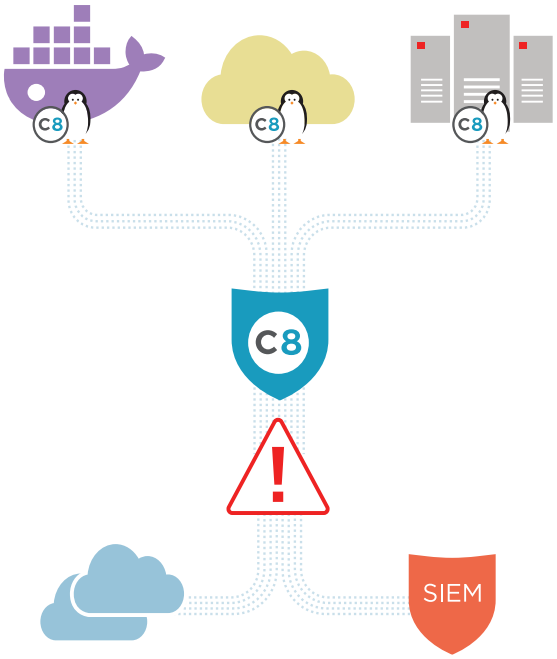
CAPSULE8

PRODUCT BRIEF

Capsule8 Enterprise Linux Protection

Detection and Resilience for Linux Infrastructure in Any Environment

- **Gain Linux detection** with coverage informed by decades of experience exploiting the Linux kernel
- **Protect cloud-native infrastructure** with detection built for the unique threat models of containers and cloud systems
- **Level up system resilience** by stopping attacks and minimizing incident impact
- **Make Ops happy** with protection architected to minimize overhead and support uptime and reliability



The modern enterprise is no longer solely end-user systems or legacy, on-premises servers, and security teams must adapt their approaches. To keep up as technology modernizes around them, security teams need to protect and respond to incidents in all infrastructure environments while supporting speed, stability, and scalability.

Capsule8 Protect is an **enterprise infrastructure protection** solution that stops attacks on Linux systems. It enables teams to immediately detect unwanted activity, gain systems resilience to support operations, and uphold security across all environments. Capsule8 Protect maximizes your team's detection capabilities with coverage informed by decades of Linux exploitation experience, ensuring unwanted attacker and developer behavior is covered. Using kprobes and perf to collect system telemetry via distributed agents, Capsule8 Protect works on **any system at any scale** – in public or private cloud, containers or VMs, on-prem bare metal, and across different kernel versions and Linux distributions.

Capsule8 Protect helps teams achieve protection parity across their enterprise infrastructure, no matter their mix of legacy and cloud-based systems. It provides:

- **Insight into unwanted activity,** collected by looking at attack chokepoints in the kernel, system operations reflecting risky developer activity, and customizable file- related actions, enriched into incident views for immediate and digestible alerting
- **Automated resilience** capabilities that facilitate incident response and system stability by immediately mitigating unwanted activity and reducing blast radius
- **Flexible integration** with orchestration, workflow, SIEM, cloud storage, and incident response tools, as well as differing kernel versions and Linux distributions
- **Ops-friendly** architecture that preserves system uptime and reliability by enabling resource limits (including CPU and network) and running without a kernel module

Capsule8 Protect is defining **modern enterprise protection** by finding and stopping attacks and other unwanted activity on Linux systems, including:


Risky developer activity and disabling of native Linux security mechanisms


Privilege escalation attacks and abuse of privileged access


Remote, interactive shell sessions


Container attacks and escapes


Memory corruption, ROP, and attempts to execute shellcode


Harvesting cloud metadata to impersonate infrastructure


Execution of newly-created files


Loading of kernel modules

Try Capsule8 Protect now

Request a demo: **capsule8.com/demo**

For more information:
info@capsule8.com
capsule8.com
@capsule8