CAPSULE8

Capsule8 Protect

Secure your production systems with visibility and detection built for Linux.

Capsule8 Protect secures your enterprise Linux infrastructure, from cloud-native to on-prem data center environments and everything in between. By providing deep visibility and threat detection at runtime into your containers, serverless, and production workloads, Capsule8 Protect enables your organization to innovate and grow with confidence while ensuring security and compliance.

CAPSULE8 PROTECT HELPS YOU,

Prevent expensive incidents in business critical systems

Attack on your production infrastructure can impact your SLAs, customer experience and reputation. Capsule8 provides detection in breadth and depth by monitoring for malicious behavior and indicators of attack in real-time to avoid business disruption.

Gain deep runtime visibility

Observability during runtime at the file, process, user and network activity level helps you plan for and build resilience. Capsule8 provides you security relevant contextual data to accelerate response and rich telemetry to perform investigations and forensics.

Avoid disruption to cloud-native infrastructure

With the short-lived nature of cloud-native workloads, real-time visibility and detection on a per instance basis is critical to avoid disruptions. Capsule8's detection is built on threat models enumerated specifically on your containers, orchestrators, serverless and other cloud workloads.

Align security and ops with performance-preserving protection

Monitoring and detection in your production infrastructure can raise stability and uptime concerns from your Ops team. Capsule8's ops friendly architecture ensures security is also performant.

Securely transform your infrastructure

Your organization could be in the middle of digital transformation with increased cloud adoption, or your infrastructure is already cloud native and expanding to Serverless and next-generation technologies; Capsule8 protects your infrastructure as it looks today and where it will evolve in the future.

- Lightweight distributed agents designed for uptime and stability to support modern operations teams
- Protection built for performance with configurable resource utilization
- Security for on-prem to cloud-native; bare metal to Serverless workloads
- Actionable alerting with flexible integration into your existing automation, orchestration, log management and incident response tooling
- Telemetry to support investigations and threat hunting

TRY CAPSULE8 PROTECT

REQUEST A DEMO:
CAPSULE8.COM/REQUEST

FOR MORE INFORMATION:
INFO@CAPSULE8.COM

Why Capsule8?

PURPOSE BUILT FOR LINUX

Detections built by Linux security experts with decades of Linux exploitation expertise for attacks specifically targeting any Linux systems at any scale. Sensors can be deployed on any platform or location running on Linux including cloud-native workloads, multi-cloud and legacy environments.

"We wanted a comprehensive host-based intrusion detection and response system that is capable of giving us deep visibility into what is happening within our environment as well as capability to respond in a systematic way to potentially malicious behavior. Capsule8 provides us with a powerful set of fundamental building blocks for hardening our security posture through its standard detection and custom detection capabilities that we can write."

Adedayo Adetoye
SENIOR MANAGER SECURITY ARCHITECTURE & ENGINEERING
MIMECAST

DEEP VISIBILITY AND DETECTION

- Comprehensive threat detection that looks for malicious behavior and indicators of attack to detect live exploits with high fidelity.
- Monitoring security relevant system activity and detailed contextual information provide deep visibility into your workloads at runtime.
- Configurable and customizable policies to cover threat models unique to your attack surface.

CLOUD-NATIVE SECURITY

- Detection for container, serverless and orchestrator specific threat models ensure that security is also reliable and scalable with your cloud-native infrastructure.
- Agent uses native Linux features such as Kprobes and perf to provide visibility into each instance of your container and serverless workloads.

INTELLIGENT INVESTIGATIONS AND FORENSICS

- Rich telemetry enables you to expedite response and reduce time to recovery.
- Available in Apache Parquet format, queryable telemetry can be stored in cloud or on-premise storage systems and accessed using plug-ins built for Athena, BigQuery, Presto and Snowflake.

FLEXIBLE INTEGRATION INTO YOUR WORFLOWS

- Capsule8's on-premise or SaaS console enables your security operations teams to monitor, respond and investigate alerts.
- One-click and API based approach enables flexible integration with your alert management systems, logging and orchestration tools, SIEMs and big data stores.

ARCHITECTED FOR PERFORMANCE AND UPTIME

- Configurable limits on CPU, memory and event rate guarantees our production systems stay performant.
- Agent runs from userland instead of kernel, reducing the need to recompile or reboot your host while upgrading kernels.
- Distributed agent architecture detects close to source avoiding expensive network bottlenecks unlike AI/ML based models which rely on phoning home data.

ACTIONABLE COMPLIANCE

- Out of the box and configurable policies that help meet IDS/IPS, FIM, and anti-virus use cases across a broad spectrum of compliance standards such as PCI, HIPAA, SOC2, FedRamp.
- Audit trail and detailed contextual information enable you to take appropriate action in addition to being alerted when policies go out of compliance.

AUTOMATED RESPONSE

- Configurable policies enable your security response teams to automatically disrupt an attack once detected.
- Automated actions definable by workload and policy type allows you to develop risk based strategic responses.