CAPSULE8

Capsule8 Protect

High-Performance Attack Protection for Linux Production Environments

Protecting your Linux production environment is a daunting task even for the most seasoned security teams. Despite investing in better analytics, the SOC continues to drown in alerts. Because source data doesn't have high fidelity, the vast majority of alerts are false-positives, and the data doesn't provide enough context for proper forensic investigation. By the time you uncover true attacks, you've already been exposed. Making the challenge even greater, traditional security solutions don't support a mix of cloud-native and bare metal infrastructure forcing security teams to look at discrete approaches for protecting different parts of their production environments.

The challenge of securing the production infrastructure brings its own set of challenges for operation teams. Operations desires quality detection in production but are concerned about the performance impact that conventional security approaches require. Effective security can't come at the expense of a high performance network.

Enter Capsule8:

Capsule8 is the only company providing high-performance attack protection for Linux production environments -- whether containerized, virtualized, or bare metal. Capsule8 liberates SecOps from managing a high volume of manual tasks, while being safe for even the busiest workloads, on the busiest networks.

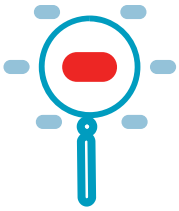
Capsule8 Protect delivers the key capabilities needed to modernize your security operations:

Real-Time Attack Protection for Linux Production

Capsule8 Protect uses distributed, streaming analytics combined with high-fidelity data that detects and responds to attacks the instant they're attempted. This real-time approach allows our customers to respond to attacks before they have costly consequences.

Detection Force Multiplier

Capsule8's approach includes a Detection Force Multiplier which delivers high-fidelity data and is continuously updated by a team of security experts to uncover the latest zero-day attacks. This approach includes highly technical methods for detecting indicators of common exploitation techniques, while still providing flexible policy-based detection (such as file integrity monitoring). As a result, a customer's typical flood of alarms is reduced to a trickle of meaningful alerts around actual exploits.

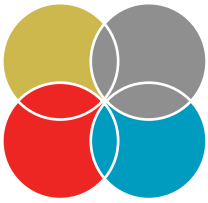


Low Volume, High Value Data

Capsule8 Protect provides relevant, contextual information that makes it easy to perform investigations that determine why alerts fire, and what an attacker does after an attack lands.

Automated Response

Customers can strategically (and automatically) kill attacker connections, restart workloads, or immediately alert an investigator upon initial detection. Capsule8 Protect helps customers respond to attacks in real-time, before they take effect. This eliminates the costly and time-consuming cleanup process that follows an attack or breach.



Easy Integration with Existing Systems

Capsule8 Protect is infrastructure- and cloud-agnostic. We provide seamless, easy-to-deploy detection across the entire infrastructure, with support for containers, VMs, bare metal, and hybrid deployments (i.e. Kubernetes, VMware, and Docker). Our API is fully extensible for easy integration into existing systems and can easily interoperate with backend workflows, allowing customers to make the most of their security investment, such as SIEMs, log analytics tools (such as Splunk and ELK Stack), and forensics tools. Our API gives you full access to your data, wherever you want it.

Importantly, Capsule8 Protect ensures that there is no risk to your production environment. Using a variety of techniques to ensure that the solution will not have an undue impact on production, Capsule8 Protect is easy for your Ops teams to manage.

No Kernel Module Needed

Capsule8 Protect runs outside the operating system's kernel and collects kernel-level data without the need of a kernel module. This approach ensures no risk to stability in production (both servers and networks).

Resource Limiter

Capsule8 Protect employs a resource limiter that enforces hard limits to system CPU, disk and memory, with an intelligent load-shedding strategy. This ensures minimal performance impact to hosts and networks.

Distributed Analytics

Unlike network-based security tools, our distributed approach to analytics pushes computation as close to the data as possible. This assures the lowest possible impact to even the busiest of networks.

Simple deployment and maintenance

Capsule8's agent is a single static Go binary that is portable and easy to install and to update through a wide variety of orchestration mechanisms, including Puppet, Ansible, Kubernetes, etc. Our system works on-premise, in the cloud (including multicloud), or in a hybrid environment. This ensures simple deployment and maintenance.

Safe For Ops

Capsule8 performs across even the most demanding and complex Linux production environments. Only small amounts of security-critical telemetry data to be shared over network. This further ensures no significant operational risk or undue impact on production. It will be easy for ops teams to manage.

Request a demo: info@capsule8.com

CAPSULE8

About Capsule8

Founded in fall 2016 and headquartered in Brooklyn, NY, Capsule8 is the only company providing high-performance attack protection for Linux production environments -- whether containerized, virtualized, or bare metal. Capsule8 frees-up SecOps teams, while being safe for even the busiest workloads, on the busiest networks. Founded by experienced hackers and seasoned security entrepreneurs, and funded by Bessemer Venture Partners and ClearSky, Capsule8 is making it possible for Linux-powered enterprises to modernize without compromise.

Learn more at: www.capsule8.com.