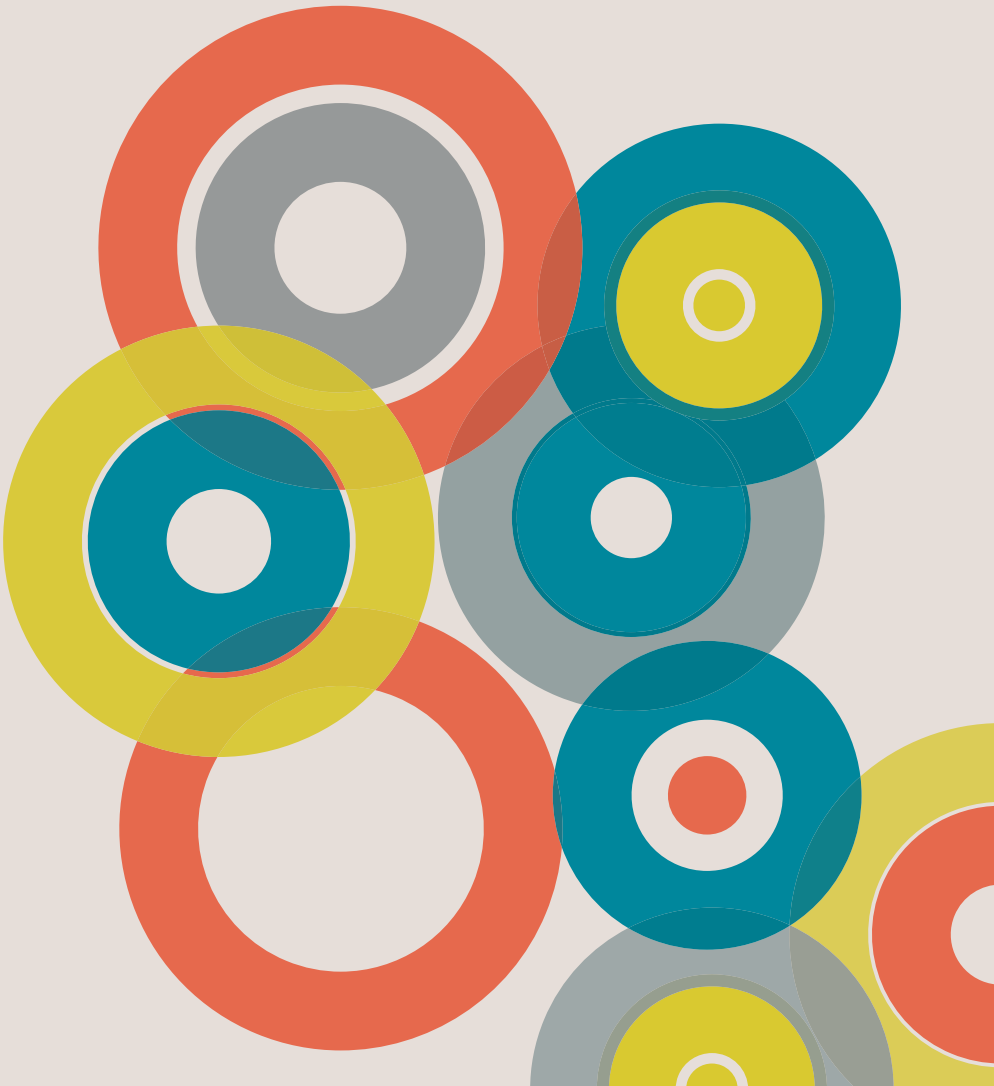
CAPSULE8

An Overview of Capsule8 for Operations

A Capsule8 Primer



Purpose

This primer describes how Capsule8 has been architected to alleviate and mitigate concerns raised by operations stakeholders charged with optimizing the performance of production infrastructure.

Introduction

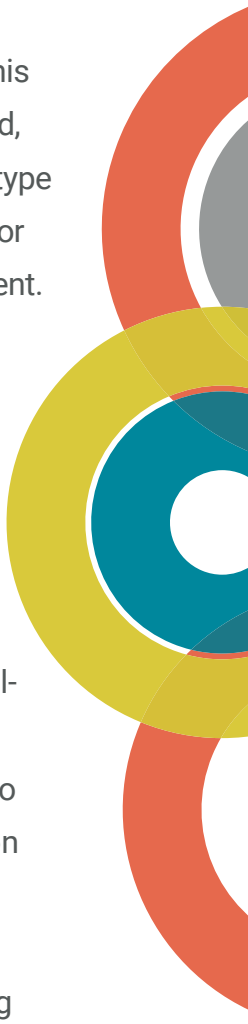
Capsule8 provides high-performance attack protection for Linux production environments — whether containerized, virtualized, or bare metal. Using distributed, streaming analytics combined with high-fidelity data, Capsule8 detects and responds to attacks the instant they're attempted. Capsule8 recognizes that deploying security in production raises concerns for operations teams who are charged with ensuring that network performance in not impacted. To that end, Capsule8 has been designed to balance and monitor both security and operational needs to ensure optimal performance of both.

This primer discusses Capsule8 in the context of stability, performance, and maintenance related to use in Linux production environments.

Simple to deploy and maintain

The Capsule8 agent is a single, static Go binary, that is portable, easy to install and update leveraging a wide variety of orchestration or configuration management tools, including Chef, Puppet, Ansible, Kubernetes, and other popular tools. Capsule8 works on-premise, in the cloud, on bare metal, in a containerized environment, or any combination of these types of environments.

When it comes to maintenance and staying up-to-date on detection, Capsule8's team of security and data scientists constantly develop detections for classes of exploitation. This means you don't need to update a signature library every time a new exploit is discovered, and that protections are in place for novel, unknown behaviors. The need to update this type of detection is far less frequent than typical tools that update for specific vulnerabilities or exploits, as attackers inventing new techniques or tactics for a given exploit is a rare event.



Once deployed and optimized to protect your unique workloads, Capsule8 can be maintained through minor, incremental efforts.

Imposes no risk to system stability

Capsule8 runs in userland (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 for servers and networks, which avoids a typical barrier to deploying protection in Linux production environments. This allows for the production workload to continue to execute where Capsule8 can still instrument data in a non-intrusive manner, not impacting the inline execution of the workload. Additionally, the lack of a kernel module does not jeopardize the license / support of the operating system by the OS provider and does not require the kernel to be recompiled.

Capsule8 was architected from the core to be independent from your systems.

Tailor to your environment

Everyone's production environment is different, so Capsule8 gives users the power to mold their protection to suit their specific needs. Capsule8 is cloud metadata-aware, making it easier to define and customize where specific detection / protection capabilities are enabled. If you're using containers, our platform dynamically scales as your container usage does -- that is, Capsule8 scales automatically as your container deployment scales.

Built-in automatic response functionality can immediately disrupt an attack before it takes hold. With a goal of optimizing security while minimizing interruptions to the Operations team, customers can define how to respond: automatically kill attacker connections, restart workloads, or immediately alert an investigator. This means dangerous activity can be shut down before it causes an outage or other disruptive incident in production. Automated attacks also allow for an audit trail to be generated even if the attack is shut down so security operations teams can learn from what took place.

Capsule8 can be customized to your production environment, scaling as you do and responding as you would.

Capsule8 was designed with performance in mind

The Capsule8 platform can be deployed to as many hosts as you need, however large the scale of your production systems. Our distributed approach to analytics pushes computation as close to the data collection as possible, ensuring minimal impact to even the busiest of workloads on the busiest of networks.

Capsule8's agent contains resource limiting capabilities, giving you the ability to customize the prioritization of CPU and memory resources. Capsule8 also contains an intelligent load-shedding feature which allows you to set event rate limits and to customize a telemetry collection backoff policy. The goal of both is to ensure your production applications take precedence over security data collection.

Lastly, you can configure Capsule8 to detect any attempted tampering of the Capsule8 system or its configuration files as it runs – removing any worry of this from the DevOps team. These strategies include kernel payload detection, detecting execution of BPF programs, loading kernel modules, or observing interference with kernel protection mechanisms like AppArmor and SELinux.

Capsule8 was architected to be self-monitoring, self-managing, and self-protecting.

Easily integrates with existing SecOps and DevOps systems

Because Capsule8 doesn't want to force you to learn another security tool, you can integrate alert data into your existing SecOps and DevOps systems, tools, and processes -- including SIEMs like Splunk, Logrhythm, or homegrown solutions already staffed to review alerts. Capsule8 supports logging alerts to a file with log rotation, printing alerts to stdout so they may be picked up by logging solutions (such as sysLog), and sending alerts to an S3 bucket or Google Cloud Storage to be picked up for analysis .

For those who want a dedicated view for Capsule8, you can choose to install the Capsule8 Console UI for investigation and/or alert consumption. The Console provides system and alert visualization as well as exploration -- insights into what potential attacks have taken place as well as any responses initiated. This helps teams more quickly conduct investigations, querying (real-time or in the background) historical

telemetry and alert data with the ability to export query results into existing user tools commonly used for additional analysis. Information that can be aggregated within the Capsule8 console includes full visibility into process lineage, and so on.

Capsule8 complements your existing collection of security tools, and conforms with established processes and procedures.

Provides multiple forms of compliance

Capsule8 can help you achieve and enforce a PCI compliant Linux production environment all within a single solution. Because Capsule8 can be deployed in heterogeneous, hybrid production environments, enterprises can shift from multiple legacy controls to a single solution that performs well on the busiest workloads and networks.

Capsule8 also satisfies compliance requirements in Intrusion Detection and Intrusion Prevention systems (IDS/IPS), File Integrity Monitoring (FIM), and Anti-Virus (AV) — meaning Capsule8 can again replace various point solutions with a single product. Capsule8 protects customers better than all the legacy solutions combined, dramatically reducing false positives, and removing performance risk in a way that makes operations teams happy.

Your enterprise can shift to a single, simple, performant solution from multiple legacy controls and help achieve a compliant Linux infrastructure.

Conclusion

With Capsule8, operations teams can support SecOps's detection configuration efforts by making sure performance is in balance with protection. Operations teams don't need to be concerned with system stability or learning new tools in which to manage higher-fidelity, lower-volume alerts; staff can simply integrate alert data into existing tools, such as SIEMs. Lastly, the Operations team's burden of deploying and maintaining tools into their environments such as IDS/IPS, FIM, and AV can be replaced by a single solution from Capsule8 that will help them achieve compliance requirements while securing their production environment

For more information,
visit capsule8.com.