CAPSULE8

Real-Time, Zero-Day Attack Detection at Scale

Capsule8 is the industry's only real-time, zero-day attack detection platform capable of scaling to massive production deployments. Capsule8 delivers continuous security across your entire production environment — containerized, virtualized and bare metal — to detect and disrupt attacks as they happen.

CAPSULE8

Delivering protection for modern production environments

REAL-TIME DETECTION AT SCALE

Capsule8 utilizes distributed, expert-driven analytics to detect attacks in real time. The result is that an organization's typical flood of alarms and false positives reduce to a trickle of high value, high context alerts of real attacks.

And, unlike conventional detection approaches that don't scale, Capsule8 relies on distributed architecture that can scale detection to tens of thousands of nodes — without impacting performance.

CLOUD NATIVE & LEGACY SUPPORT

Capsule8 supports both orchestrated and non-orchestrated workloads.

Capsule8 deploys as easily in a Kubernetes orchestrated environment through cloud providers such as AWS, GCP or Azure, as well as bare metal environments deployed with your operations tools of choice such as Ansible, Puppet, Chef or SaltStack.

INTELLIGENT INVESTIGATION

Capsule8's distributed telemetry makes it easy to perform forensic investigations on historical data, without significant impact to network performance or storage.

BUILT FOR PRODUCTION

When your network is under heavy load, Capsule8 responds to ensure overall performance isn't impacted. Moreover, Capsule8 works without deploying any kernel modules or high-risk components.

It deploys alongside your infrastructure, not as a SaaS solution, giving you full control of your data and eliminating the risks of dissemination, deletion, or corruption of data by third parties.

AUTOMATED DISRUPTION

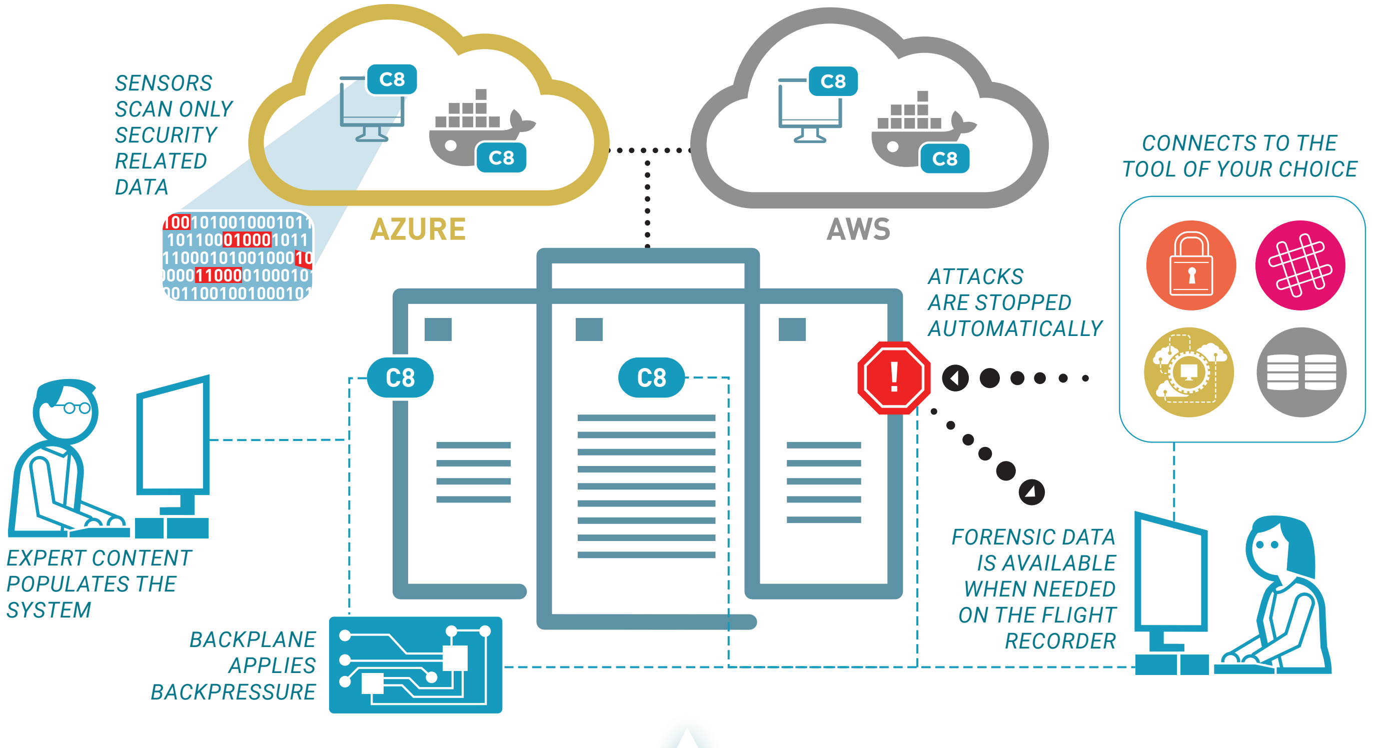
Capsule8 can go beyond detection and enable you to automatically disrupt an attack once detected.

For instance, customers can strategically (and automatically) kill attacker connections, restart workloads, or immediately alert an investigator, immediately upon initial detection.

EASY THIRD-PARTY INTEGRATION

Capsule8's API-first approach allows simple integration with alert management systems, communication tools, SIEMs, orchestration tools and big data stores.

HOW CAPSULE8 WORKS


SENSORS SCAN ONLY SECURITY RELATED DATA
C8
AZURE
AWS
CONNECTS TO THE TOOL OF YOUR CHOICE
ATTACKS ARE STOPPED AUTOMATICALLY
EXPERT CONTENT POPULATES THE SYSTEM
BACKPLANE APPLIES BACKPRESSURE
FORENSIC DATA IS AVAILABLE WHEN NEEDED ON THE FLIGHT RECORDER

Capsule8 Lightweight Sensors
Deployed on Linux hosts running workloads that can span on-premises data centers and public or private clouds.

The Capsule8 "Flight Recorder"
Runs alongside these sensors to record telemetry events locally.

Capsule8 Detection
Small amounts of security-critical data are streamed to nearby Capsule8 Detect analysis instances, which detect zero-day attacks in real time. When an attack is detected, Capsule8 can immediately disrupt that attack before it takes hold.

The Capsule8 Backplane
Includes a real-time messaging bus that connects all sensors wherever they are deployed to stream requested real-time and historical events from the Flight Recorder.

The Capsule8 API Server
Provides a consistent interface that allows organizations to manage all data as part of their security infrastructure.

The Capsule8 Console
Gives organizations the option to use a Capsule8-specific dashboard with an actionable menu and filters to easily tap into Capsule8's capabilities.

Modernize Without Compromise

Visit **www.capsule8.com**
Contact us at **info@capsule8.com**

CAPSULE8