INTEZER PROTECT

Protect your cloud infrastructure against the root cause of cyber attacks: UNAUTHORIZED CODE

INDUSTRY LEADING THREAT DETECTION WITH NO MANUAL CONFIGURATION OR OVERHEAD FOR YOUR TEAM

Intezer Protect is a **Cloud Workload Protection Platform** (CWPP) that defends your cloud infrastructure against unauthorized and malicious code. Revealing the "genetic" origins of all applications running on your systems, Intezer provides full visibility in runtime and enables you to adopt a **Zero Trust Execution** strategy without the operational overhead.

Zero Trust Execution Meets Low Overhead

GCP AWS AZURE

PROTECT YOUR AWS, AZURE, GCP OR PRIVATE CLOUD ENVIRONMENTS

against the **root cause of all cyber attacks:** unauthorized and malicious code.

ADOPT A ZERO TRUST EXECUTION STRATEGY

without the high maintenance, disrupting the agile CI/CD pipeline or downgrading your servers' performance. Ensure all code running on your cloud infrastructure is under your control and solely from trusted origins.

ALLOW YOUR ORGANIZATION TO CONTINUOUSLY INNOVATE

while knowing the entire spectrum of your workloads—including Virtual Machines, containers, Kubernetes and Open Shift instances, and more—is secure.

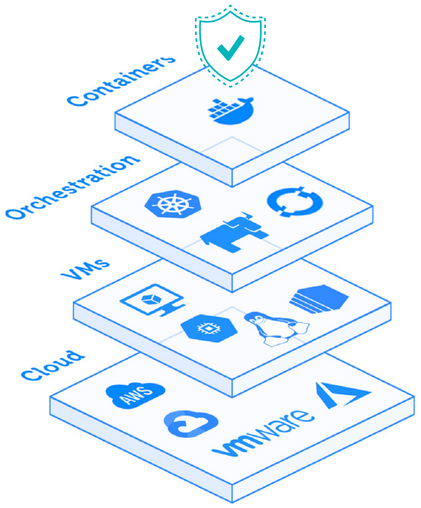
PCI DSS COMPLIANT HIPAA AICPA SOC

INTEZER PROTECT

Advantages

Secure entire cloud-native stack

and Linux servers



Defend against modern and evolving attacks

Our in-memory Genetic Software Mapping capabilities defend against a wide scope of attack vectors

- Malicious code
- Vulnerability exploitation and other fileless threats
- Unauthorized or risky software
- Suspicious shell commands and administrative activity

All recommended IaaS security controls

under one platform

App Control
Memory protection
EDR-like visibility
Anti-malware
System integrity

Full visibility

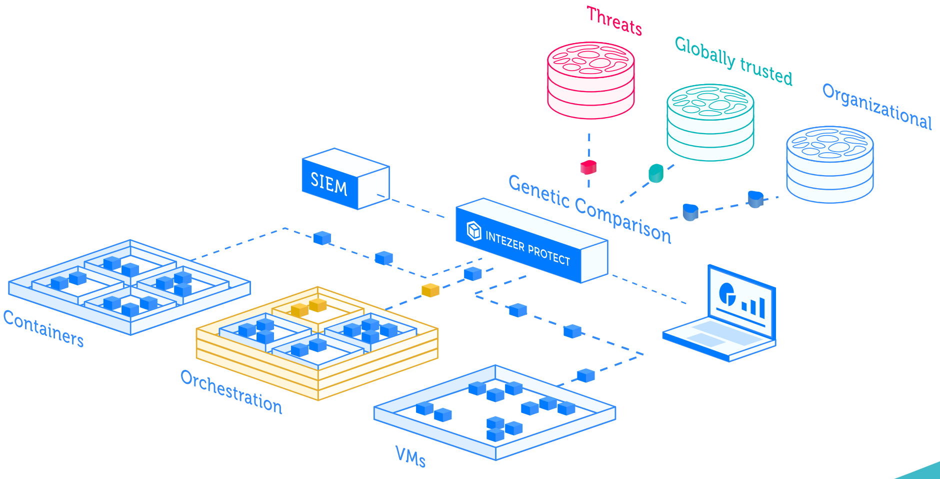
and control over all code and applications running in your environment

Low overhead

Produce only high-confidence alerts with no manual configuration, rules, or policies required

How it Works?

We create a genetic profile of your workloads and continuously monitor for new code running in memory. Any detected deviation from the baseline is genetically inspected which allows us to alert you only on deviations that present true risk, rather than natural deviations such as legitimate software upgrades that don't require a response.



Protect your Cloud Workloads

Get your Free Online Trial