BENEFITS

Breach Detection

Discovers attacks that are invisible to standard security products

Total Visibility

Unparalleled visibility into activity inside the data center, including containers

Total Scalability

Scales to any traffic load inside the hypervisor or server and throughout the entire data center

Rapid Analysis and Response

Attack analysis and detection of attacker's footprint provides complete and detailed insight into the breach details

Remediation

Identifies the source of attack and attacker tools; Quarantine of infected files and machines

Lower Cost of Ownership

Simplifies protection and management by reducing the time it takes to detect a breach and respond to it

Flexible Deployment Options

Tight integration with Software Defined Data Center controllers and orchestration components, public clouds and bare-metal environments

All Data Center-Based Technologies Should Be Protected

Data centers are home to critical corporate data and business processes, making them a lucrative target for cyber attacks. The modern data center is built on various virtualization technologies including containers, which include the application and all of its dependencies, while sharing kernel with other containers. Docker provides containers that run as isolated processes in the user space on a host operating system. Docker containers are not tied to any specific infrastructure and can run on any computer, infrastructure or cloud. Containers provide an efficient way to shorten the deployment process and while it has many built-in infrastructure protection capabilities, the applications running on Docker are still as insecure as other applications deployed with other types of technologies. Inside the data center, Docker containers may store or provide access to the most valuable assets.

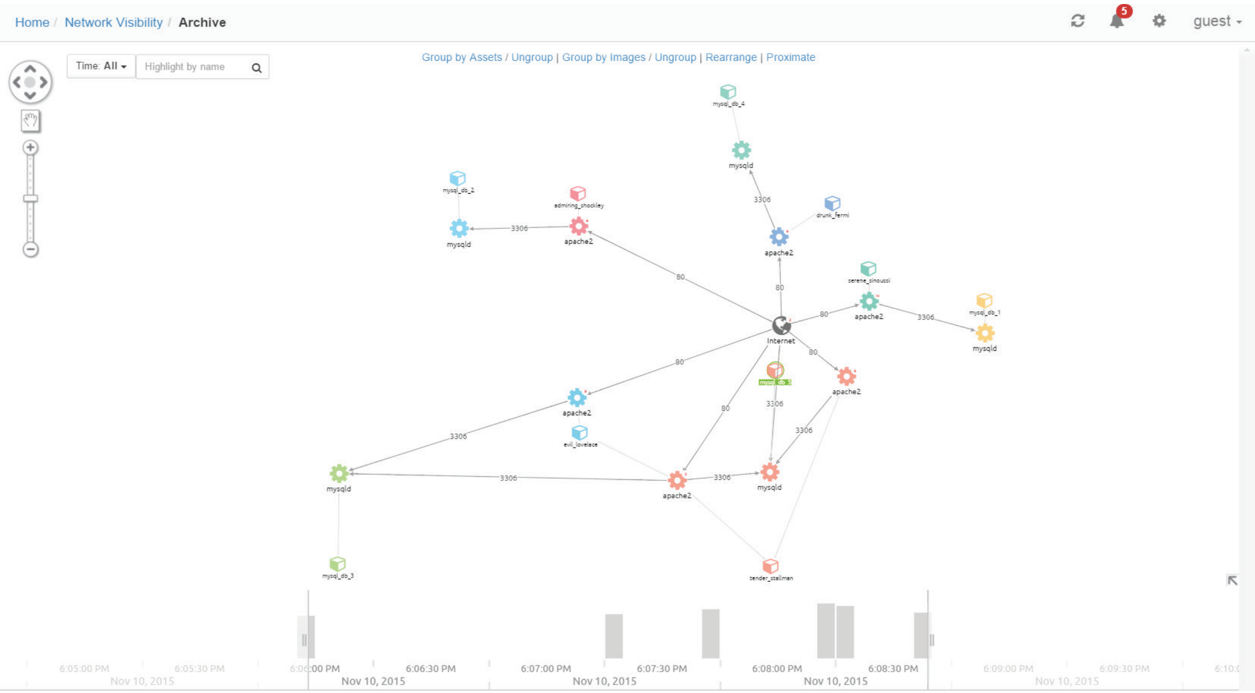
Perimeter-Based Security Controls Can't Protect the Internal Data Center

Once inside a data center, intruders are very hard to detect and respond to. According to multiple researches, it typically takes many months to discover a breach, detect its source and remediate.

The GuardiCore Data Center Security Suite helps address this interior data center security challenge by providing visibility into data center activity, scaling cutting-edge security techniques to keep pace with east-west traffic rates. Using multiple detection methods, it exposes attackers, provides quick insights into the nature of the attack and responds to it in real time.

Supporting Distributed architecture per hypervisor, server or container, the Suite offers full coverage of all traffic inside data centers and scales to very large network sizes and traffic rates, with low impact on hypervisor/server performance.

GuardiCore also provides data center visibility to support and reflect containers in a dedicated way, enabling IT personnel to effectively monitor, maintain and troubleshoot all Dockerized environments in a highly granular manner, including the tracking of process-to-process communication between any two containers.



About GuardiCore

GuardiCore is a leader in Internal Data Center Security and Breach Detection. Developed by the top cyber security experts in their field, GuardiCore is changing the way organizations are fighting cyber attacks in their data centers.

More information is available at www.guardicore.com