GuardiCore

GuardiCore Centra™ Security Platform

Internal Data Center Security and Breach Detection

Perimeter-Based Security Approach for Data Centers Has Proven Inadequate

Data centers are home to critical corporate data and business processes, making them a lucrative target for cyber attacks. Once inside a data center, intruders are very hard to detect and respond to. According to multiple research reports, it typically takes many months to discover a breach, detect its source and remediate.

> *According to multiple researchers, it typically takes many months to discover a breach, detect its source and remediate.*

The GuardiCore Centra™ Security Platform helps address this interior data center security challenge by providing a unique combination of process-level visibility, threat deception, semantics-based analysis and automated response to detect, investigate and mitigate data center threats in real-time. Distributed per hypervisor or server, the Centra Platform 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.

How it Works

GuardiCore employs a lightweight, distributed component across the data center that monitors all connections using multiple detection methods. Unsuccessful connections are transparently rerouted to a high-interaction deception engine for investigation while successful connections are analyzed for malicious attributes. Centralized management performs semantic analysis of connections and attacker's activity and alerts on any deviation from authorized and expected behavior. It detects humans as well as APTs and bots at the stage of lateral movement, providing the ability to search for the full spread of the breach and enabling automated mitigation and remediation of infected servers.

GuardiCore Reveal™, part of the Centra Security Platform, discovers and tracks process-level activity across applications and correlates it with network events, providing a dynamic visual map of the entire data center network. It detects and reports on suspected anomalies and incidents, providing the security administrator with a quick view of all workloads.

The GuardiCore Centra Security Platform is integrated into OpenStack, CloudStack and VMware infrastructures, and can be also installed in physical data centers and public clouds.

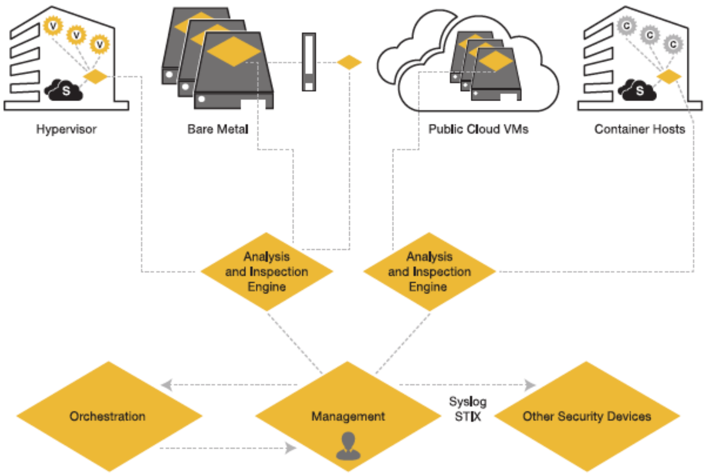
Benefits

- **Total Visibility**
  Process-level visibility into applications and workloads inside the data center.
- **Breach Detection**
  Discovers attacks that are invisible to standard security products.
- **Rapid Analysis and Response**
  Attack analysis and detection of attacker's footprint provides complete and detailed insight into the breach.
- **Remediation**
  Identifies the source of attack and attacker tools; quarantines infected files and machines.
- **Total Scalability**
  Scales to any traffic load inside the hypervisor or server and throughout the entire data center.
- **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 SDDC controllers and orchestration components, public clouds and bare-metal environments.

Designed to Protect the Modern Data Center

The GuardiCore Centra Security Platform is tightly integrated with different controllers and orchestration components for object identification and reporting. It provides full coverage of all VMs and VM-to-VM traffic, including on the same hypervisor. Designed to accommodate the most demanding environments, a 3-tier architecture is scalable to meet the performance and security requirements of data centers at any size, with very low impact on hypervisor performance.

Architecture *Using a 3-tier architecture, GuardiCore is capable of providing detection and remediation while performing under any traffic load.*



Deployment Diagram

Large scale distributed deployment *containing multiple environments, with agents forwarding traffic to analysis engines working in tandem to increase the capacity of the system. Analysis engines can be added at any time as deployment scales up. Management and analysis server can be deployed in the cloud or on premises.*

Breach detection and response *using a distributed light-weight component, installed as a Secure Virtual Machine (SVM) for VMware hypervisors and public clouds or a process for other hypervisors. It detects suspicious activity anywhere inside the data center. Once detected, this component is also used in breach mitigation and remediation.*

Analysis and inspection *engine performs deep investigation of suspicious activity, determines if an event is indeed malicious, understands its behavior and identifies the spread of the breach. Multiple analysis engines can be combined to increase the overall performance capacity.*

Reporting and alerting *using a centralized management component, providing a single point of control for the entire system, UI for the administrator and integration with security management tools including SIEM and ticketing systems.*

Deployment options

The GuardiCore Centra Security Platform can be installed on physical and virtual environments to protect your assets. Hybrid deployments are supported, enabling operational flexibility and potential growth.

Detection and remediation

Hypervisor detection engine/SVM. Tap/SPAN port for physical networks. Detection Agents for public clouds.

Browser for web console

Google Chrome 38 or later, Microsoft Internet Explorer 11, Mozilla Firefox 29 or later. Screen resolution: 1920x1024.

Management and Analysis

On premise physical or virtual appliances. GuardiCore as a service: analysis and management.

Supported Orchestration

VMware vSphere 5.5.x, VMware vCenter Server 5.5 or later, VMware NSX Manager 6.1.x, Nuage Networks, Mirantis CloudStack, OpenStack.

Supported Hypervisors

KVM, Xen, VMware ESX 5.1 or later for each server.

Supported Cloud Solutions

Amazon AWS, Microsoft Azure.

Intelligence Sharing Protocols

STIX, Syslog, CEF, Open REST API.

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**