GuardiCore Centra™ Security Platform
Advanced Security for Modern Data Centers and Clouds

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

The GuardiCore Centra™ Security Platform solves these challenges with the five critical capabilities needed to secure modern data centers and clouds: flow visualization, micro-segmentation, breach detection, automated analysis and response.

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 deviations from authorized and expected behavior. Centra detects human attackers as well as APTs and bots, 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 Centra Security Platform integrates with OpenStack, CloudStack and VMware infrastructures, and can be also installed in physical data centers and public clouds.

Highlights

- **Comprehensive Breach Detection and Rapid Response**
  Multiple methods of detection discover attacks that are invisible to standard security products.

- **Application-Centric Micro-Segmentation**
  Quickly define, monitor and enforce application-centric micro-segmentation security policies.

- **Total Scalability and Security**
  Scales to protect high-performance traffic loads inside the throughout the entire data center.

- **Secure Cloud Migrations**
  Secure workloads during migrations to virtually any data center configuration.

- **Lower Cost of Ownership**
  Simplifies protection and management by reducing the time it takes to detect a breach and respond to it.
Multiple Detection Methods Detect and Respond to Breaches Faster

IT teams are overwhelmed with responding to potential indicators of compromise originating inside the data center and need the ability to detect and respond to breaches faster and with greater intelligence. Detection methods must scale to secure a massive increase in east-west traffic rates. When a breach is detected, IT teams also need automated tools to help them understand the breach and know how to prioritize response actions—especially in dynamic, auto-scaling environments.

Centra uses multiple detection methods including patented dynamic, distributed deception, analysis of policy-based traffic flows, and reputation analysis of domain names, IP addresses and file hashes to detect breaches inside the data center faster, reduce dwell time and block lateral movements. Automatic incident analysis provides security teams with real-time information and comprehensive intelligence about attack methods so they can quickly prioritize security response actions which would otherwise involve hours of human analysis using traditional tools and techniques. Centra also automates incident response with real-time remediation of infected systems including preventing the spread of ransomware.

Dynamic Deception Snares the Attacker—Identifies Tactics, Methods and the Source

Using patented redirection and deception technologies, Centra detects lateral movement activity, which is a strong indicator of a potential breach, and dynamically redirects suspicious traffic to the GuardiCore Deception Environment for high-interaction engagement and monitoring.

Highlights

Dynamic Deception
A redirection architecture and dynamically generated live environments engages attackers and identifies their methods without disrupting data center performance.

Policy-Based Detection
Security policies at the network and process levels enable instant recognition of unauthorized communications and non-compliant traffic.

Reputation Analysis
With GuardiCore reputation analysis, Centra detects suspicious domain names, IP addresses and file hashes within traffic flows providing comprehensive breach detection.

Automated Analysis and Response
GuardiCore provides real-time incident information with high-fidelity intelligence about attack methods to help you understand the entire breach scenario and prioritize remediation resources.

“This tool is the whole package: active breach detection, deception technology, advanced analytics, forensic analysis in real time, and real-time remediation.”
Security Policies and Reputation Analysis Detects Unauthorized Communications and Spotlights Known Bad Actors

With policy-based detection, IT teams can create rules governing authorized communications between applications. Any non-compliant traffic, unauthorized communication or other policy violation automatically triggers an alert indicating an intruder may be present. This in turn initiates the investigative process to confirm and contain the threat.

Reputation analysis is aimed at identifying threats based on suspicious domain names, IP addresses and file hashes associated with known malicious activity. Reputation analysis leverages GuardiCore’s network of attack sensors and deception engines, threat intelligence feeds and the insights of our security analysts. The platform also has the ability to distinguish “negative processes” indicating the presence of an untrusted asset that warrants investigation.

Rapid Visualization and Application-Centric Micro-Segmentation with GuardiCore Reveal™

GuardiCore Reveal, a key component of the GuardiCore Centra™ Security Platform, provides process-level visibility into applications and workloads combined with granular policy definition enabling security teams to discover, visualize, control and monitor activity inside the data center. Teams gain a better understanding of applications and can detect breaches faster by identifying suspicious behavior.

GuardiCore Reveal provides complete process-to-process visibility and segmentation policy management for the entire data center, across multiple VMs and between assets (public or private).

Highlights

- **Process-level Visibility**
  Visualize all applications and their traffic, including process-to-process communications.

- **Time-Based View**
  Visualization and usage reports are based on actual traffic monitored and can be viewed in different timeframes, including historical information.

- **Breach Detection**
  Detect attacks by identifying suspicious activity between applications and processes.

- **Micro-Segmentation**
  Define and manage granular, application-aware micro-segmentation security policies down to the process level.

- **Compliance**
  Monitor all data center communications against defined policies and generate incidents for any variation.
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 Highlights

Protect and Collect
Hypervisor collectors and Guest OS agents for virtualized assets and containers in private or public clouds.

Aggregate
Virtualized aggregation servers collect and normalize data.

Manage and Analyze
Management servers and deception environments are deployed in a SaaS configuration.

Centra 3-Tier Architecture Delivers Flexibility, Scalability and Performance

Using a 3-tier architecture, GuardiCore Centra provides detection and remediation while performing under heavy traffic loads.

Support for the Modern Data Center Infrastructure

GuardiCore Centra is designed to integrate with your infrastructure.

**Orchestration**
VMware vSphere 5.5.x, VMware vCenter Server 5.5 or later, VMware NSX Manager 6.1.x, Nuage Networks, CloudStack, Mission Critical Cloud, Openstack (Vanila/Mirantis)

**Hypervisors**
KVM, XenServer, VMware ESX 5.1 or later for each server

**Intelligence Sharing Protocols**
STIX, Syslog, CEF, Open REST API

**Public Cloud Providers**
Amazon Web Services, Microsoft Azure, Oracle OPC

**Container Orchestration & Engines**
Docker

**Security Gateways**
Palo Alto Networks, Check Point Software Technologies, Cisco

**Memory and System Requirements**
Aggregator:
2 GB RAM min, 4GB RAM recommended, 2 vCPUs min, 4 vCPUs recommended, 30GB storage

Collector:
2 GB RAM min, 4GB RAM recommended, 2 vCPUs min, 4 vCPUs recommended, 30GB storage

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](http://www.guardicore.com)