GuardiCore

DATA SHEET

GuardiCore Centra™ Security Platform

Single, Converged Platform That Provides Critical Controls for Hybrid Clouds Across Any Environment

More and more organizations are moving to public clouds and, more typically, to public-private hybrid data center architectures. For all the flexibility organizations have gained, the added complexity of multiple-cloud infrastructures has multiplied the attack surface; with little or no communication controls in place, each individual server becomes an attack surface in and of itself. As a result, attackers can spend more time moving laterally – and undetected – between east-west traffic workloads.

The GuardiCore Centra Security Platform provides comprehensive security controls in a single platform that reduces security management complexity and eliminates the need for multiple point solutions in hybrid cloud environments.

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 GuardiCore Centra Security Platform provides protection for your entire infrastructure. Centra protects workloads in hybrid cloud environments that span on-premises workloads, VMs, containers and deployments in public cloud IaaS including Amazon Web Services, Microsoft Azure and Google Cloud Platform.

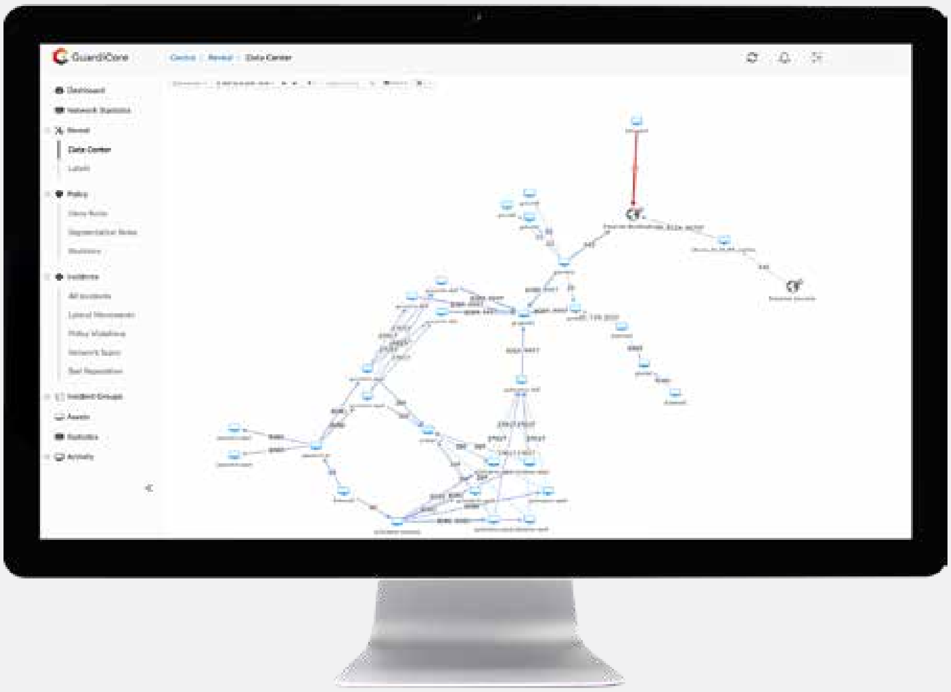
Highlights

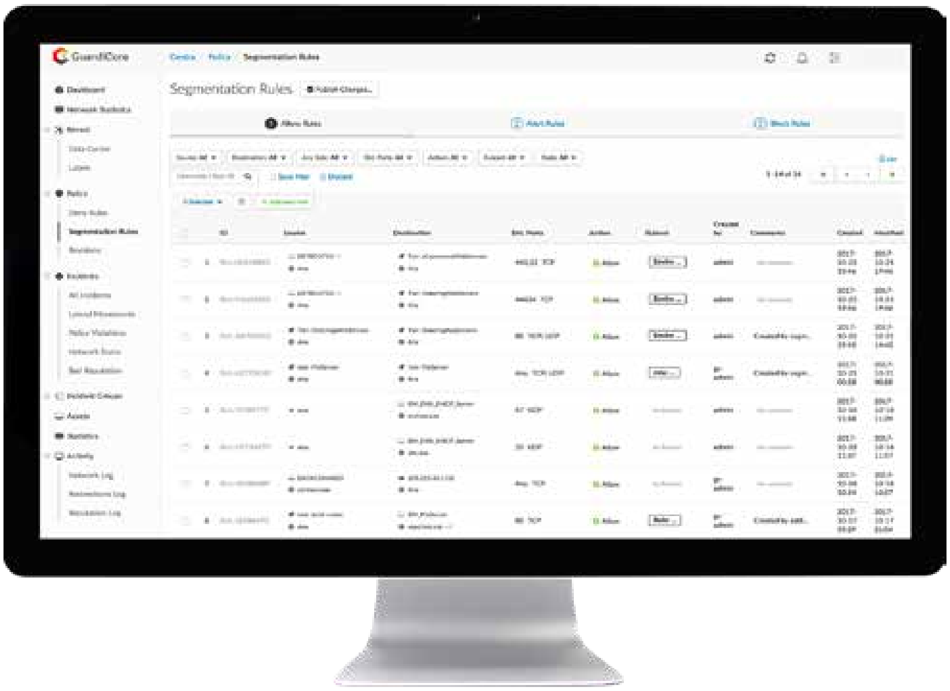
- **Flow Visualization**
  Visually map all application workloads, down to the process level.
- **Micro-Segmentation**
  Flexible policy engine simplifies creation and deployment of segmentation rules.
- **High-Interaction Deception**
  Actively engage attackers and identify their methods in real-time.
- **Reputation Analysis**
  Instantly detect suspicious domain names, IP addresses and file hashes within flows.
- **Automated Analysis**
  High fidelity attack intelligence including attackers' tools, tactics and source.
- **Incident Response**
  Attack isolation and remediation recommendations speeds incident response.

Solution Benefits

Discover and Visualize Application Flows Across the Entire Infrastructure

- Automatically discover applications and flows
- Quickly understand application behavior
- Granular visibility down to the process level



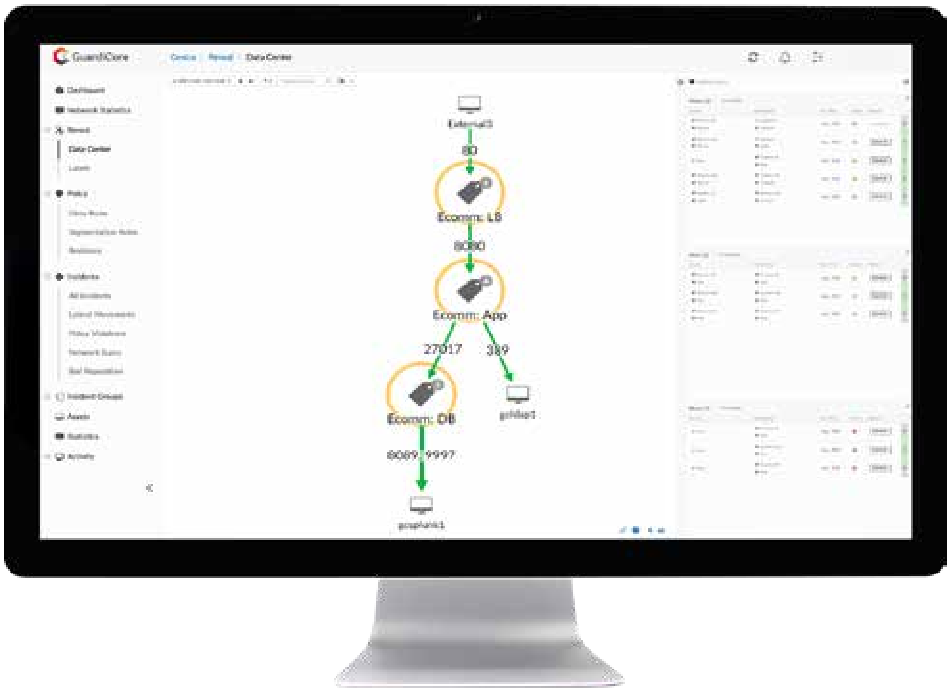


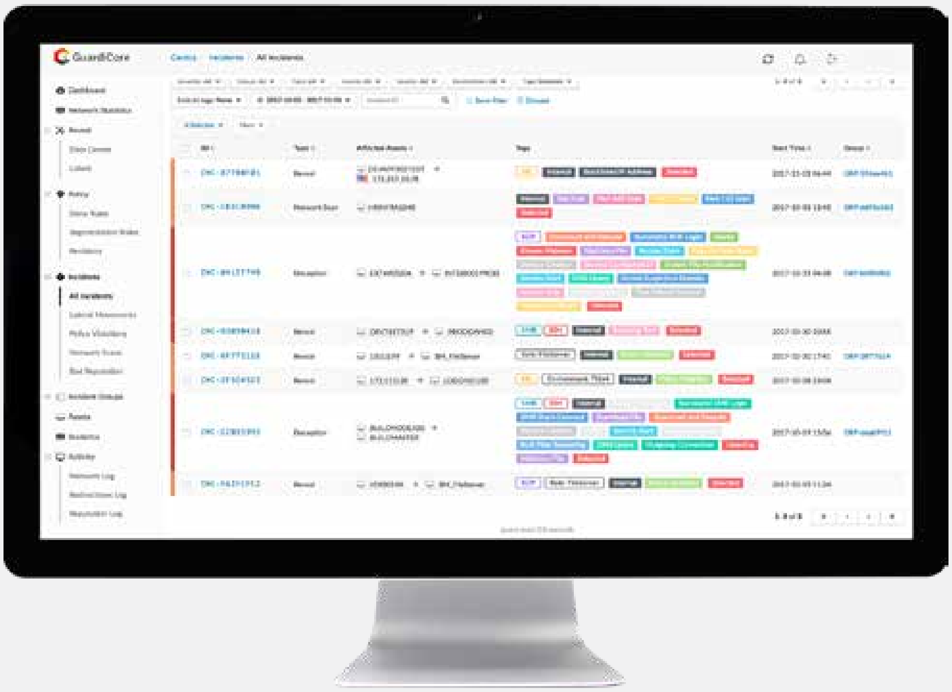
Strong Micro-Segmentation With a Flexible Policy Engine and Management

- Define segmentation policies in minutes
- Automatic policy recommendations
- Consistent policy expression across any environment

Intelligent Rule Design Helps You Refine, Strengthen and Maintain Policies

- Quickly and visually design rules based on asset labels and groups
- One-click generates suggested rules based on historical communications
- Native rule enforcement on Windows and Linux systems





Detect More Threats Faster and Respond With Greater Intelligence

- Multiple detection methods covers all types of threats
- Dynamic deception immediately traps attackers
- High-quality, in-context security incidents with mitigation recommendations to speed incident response

Protection For Your Entire Infrastructure, Built and Proven for Cloud Scale

Any Hybrid Cloud

Protect workloads in hybrid cloud environments that span on-premise workloads, VMs, containers and deployments in public cloud IaaS including AWS, Azure and GCP

Simplify Security

Simplify security management with one platform that provides flow visibility, micro-segmentation, breach detection and incident response

Enterprise Scalability and Performance

Scalable to meet the performance and security requirements of any sized environment

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

Industry Recognition

About GuardiCore

GuardiCore is an innovator in data center and cloud security focused on delivering more accurate and effective ways to stop advanced threats through real-time breach detection and response. Developed by the top cyber security experts in their field, the GuardiCore Centra Security Platform is changing the way organizations fight cyber attacks.

More information is available at **www.guardicore.com**