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.

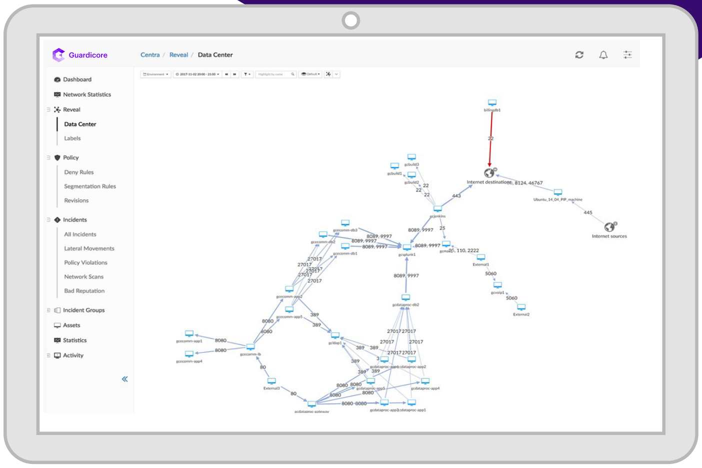
Guardicore Reveal™, part of the Centra Security Platform, discovers and tracks process-level activity across applications and correlates it with network events, providing a dynamic visual map of the entire data center network. It detects and reports on suspected anomalies and incidents, providing the 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.
- **Container Security**
  Enforce security controls throughout build, deploy, and runtime environments.
- **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.

The Most Complete Solution for Micro-Segmentation



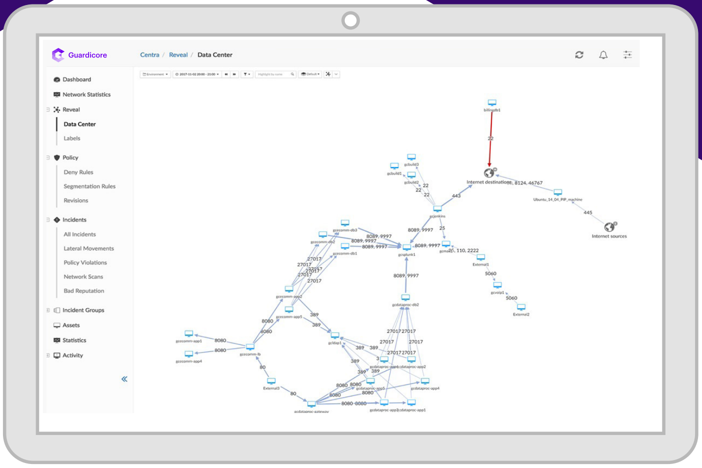
Reduce the Attack Surface, Secure Critical Applications

- **Wide Coverage:** Apply micro-segmentation policies anywhere your applications run today or tomorrow, spanning public, private or hybrid cloud environments.

- **Deep Visibility:** Application-aware visibility so you understand the full context of application dependencies before defining micro-segmentation security policies.

- **Intuitive Workflow:** A simple workflow from mapping application dependencies to suggesting and setting rules, so you understand their impact before applying to traffic.

- **Granular Policies:** Set and enforce “process-level” rules to tightly control flows between application components, resulting in the strongest security posture.



Successfully Navigate the Path to Micro-Segmentation in Three Easy Steps

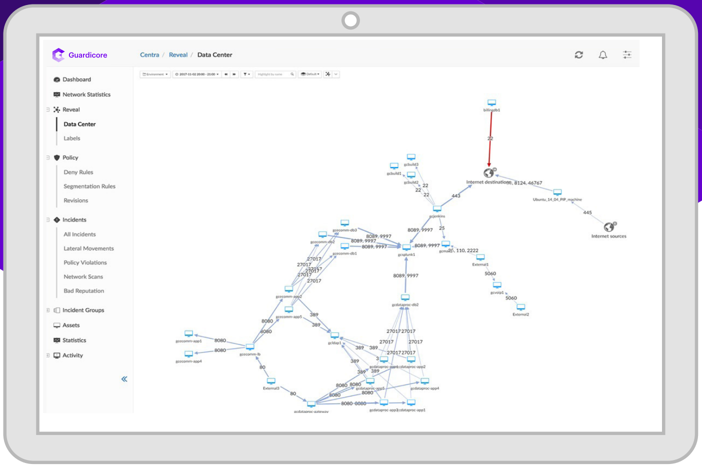
- **Reveal:** Guardicore Centra features best-in-class visibility that automatically discovers and visualizes all applications, workloads and communication flows with process-level context. This visualization, coupled with automatic importation of orchestration metadata, enables security teams to easily label and group all assets and applications and streamline policy development.

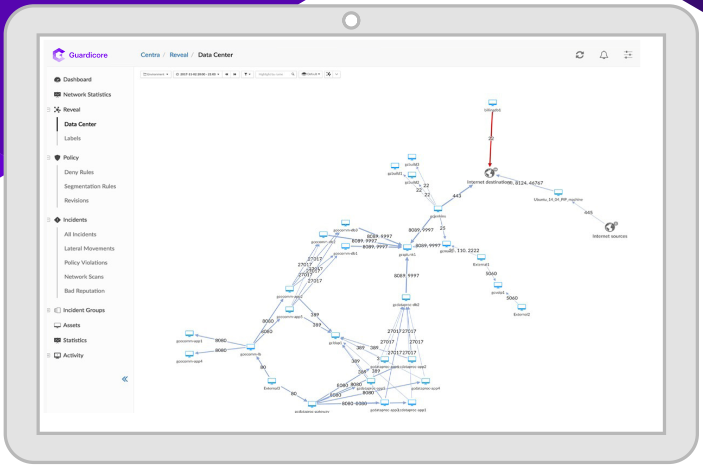
- **Build:** Guardicore simplifies micro-segmentation policy development and management. A single click on a communication flow generates automated rule suggestions based on historical observations and quickly builds a strong policy. An intuitive workflow and a flexible policy engine supports continuous policy refinement and reduces costly errors.

- **Enforce:** With the ability to enforce communication policy at the network and process level on both Windows and Linux systems, Centra maintains security regardless of operating system enforcement limitations. Integrated breach detection and response capabilities enable you to see policy violations in the context of an active breach and identify the method attack.

Guardicore

Detect More Threats Faster and Respond with Greater Intelligence





Breach Detection, Investigation and Response That's Built for the Cloud

- **Multiple Detection Methods:** Three detection methods — Dynamic Deception, Reputation Analysis and Policy-Based Detection — simultaneously form a strong security net, virtually ensuring that any live breach is caught, mitigated and contained for in-depth investigation.
- **Built for the Cloud:** Patented dynamic deception with additional methods designed for the unique requirements of the cloud provides coverage against attack vectors that other product miss.
- **Integrated Response:** Highly accurate detection coupled with actionable intelligence and exact knowhow about the attackers' tools and methods with real-time response recommendations and actions.
- **Detailed Forensics:** Incident data is presented in a human-readable fashion alongside the evidence including indicators of compromise, relevant artifacts and the identifying characteristics of human attacks vs. bots.

See the Entire Attack, Block Lateral Movements and Reduce Dwell Time

- **Detect:** Centra features multiple detection methods designed for attacks on clouds and data centers including distributed, dynamic deception which engages attackers and identifies their methods without disrupting cloud or data center performance, reputation analysis that detects suspicious domain names, IP address and file hashes within traffic flows, and policy-based detection enables instant recognition of unauthorized communications and non-compliant traffic.
- **Investigate:** Centra collects the entire attack footprint — the files and tools being used and uploaded, and the arsenal of weapons that the intruder activates — and performs deep forensics to expose user credentials, attack methods, propagation tactics and more.
- **Respond:** Accelerate incident response with automatic exports of IOCs to security gateways, SIEM and ticketing systems to block, contain and investigate attacks, single-click updates to segmentation policies to remediate traffic violations, and the ability to trigger actions on VMs — suspend, halt, disconnect or snapshot — to prevent the spread of damage from ransomware attac.

Guardicore

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
Amazon Web Services, Microsoft Azure, Oracle OPC

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 an innovator in data center and cloud security that protects your organization’s core assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security - for any application, in any IT environment.

www.guardicore.com

v. 4.0