Guardicore

DATA SHEET

# Guardicore Centra™ Security Platform

## Granular Visibility and Micro-Segmentation Controls for Data Center, Cloud, and Hybrid Cloud Environments

Enterprise IT infrastructure is evolving rapidly from a traditional data center model to cloud and hybrid cloud architectures with a mix of platforms and application deployment models. While this transformation is helping many organizations achieve greater business agility and reduce infrastructure costs, it is also creating a larger and more complex security attack surface. As the traditional concept of a network perimeter becomes less relevant, each individual server becomes a possible launch point for an attack. Attackers are responding to this shift by increasing their focus on moving laterally between east-west traffic workloads.

The Guardicore Centra™ Security Platform is a comprehensive data center and cloud security solution that delivers the simplest and most intuitive way to apply micro-segmentation controls to reduce the attack surface and detect and control breaches within east-west traffic. It provides deep visibility into application dependencies and flows and enforcement of network and individual process-level policies to isolate and segment critical applications and infrastructure.

## How It Works

Guardicore Centra collects detailed information about an organization's IT infrastructure through a mix of agent-based sensors, network-based data collectors, and virtual private cloud (VPC) flow logs from cloud providers. This information is then placed into context through a flexible and high-automated labeling process that includes integration with any existing data sources like orchestration systems and configuration management databases.

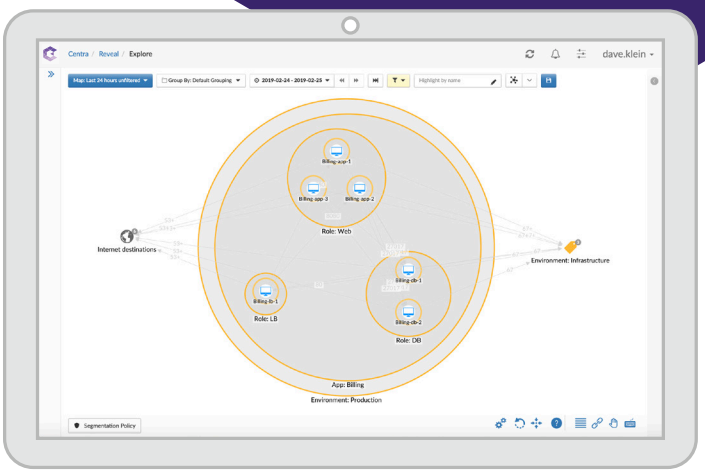
The result is a dynamic visual map of the entire IT infrastructure that allows security teams to view activity down to the individual process level on both a real-time and historical basis. These detailed insights into application behavior can then be used to create granular micro-segmentation policies quickly through an intuitive visual interface. Centra's micro-segmentation capabilities are also complemented by an innovative set of breach detection and response capabilities.

Centra provides protection for your entire infrastructure. Centra protects workloads in hybrid environments with any combination of legacy systems, bare-metal servers, virtual machines, containers, and cloud instances in Amazon Web Services, Microsoft Azure, and Google Cloud Platform.

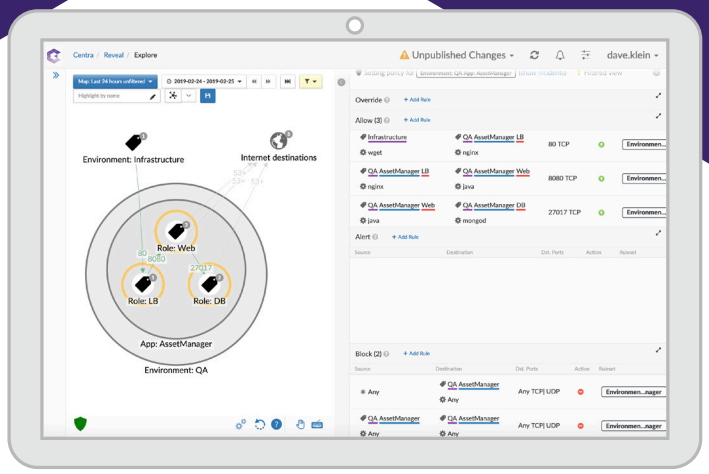
## Highlights

- **Unmatched Visibility**
  Map application dependencies and flows down to the process level with context in both a real-time and historical basis
- **Platform-Independent**
  Apply micro-segmentation to any operating system across any combination of legacy systems, bare-metal servers, VMs, containers, or cloud instances
- **Granular Policy Enforcement**
  Define and enforce L4 and L7 segmentation policies consistently across all servers and operating systems
- **Extensive Use Case Support**
  Supports the broadest set of segmentation and micro-segmentation use cases, from environment segmentation to application ringfencing and more
- **Broad Protection**
  Integrated breach detection and incident response capabilities augment micro-segmentation measures for increased protection and ROI

# Simple and Intuitive Micro-Segmentation




Guardicore Centra automatically discovers application dependencies and flows and generates a visual map to ensure full a full understanding prior to applying segmentation policies.




Directly from the visual map, administrators can quickly build application and micro-segmentation policies based on automatically generated rule recommendations and historical context.

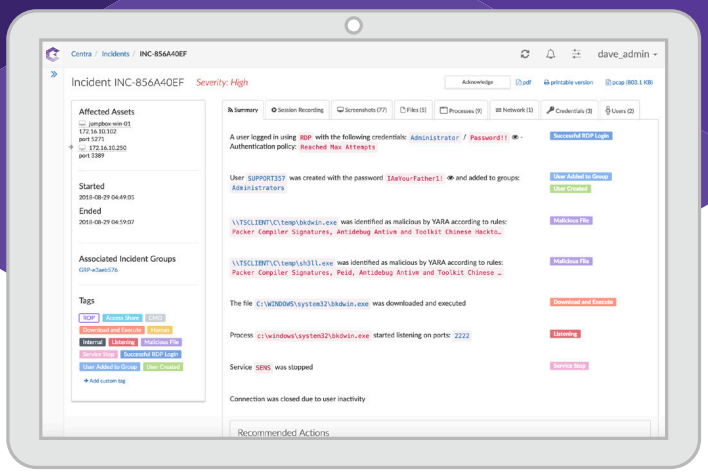
## Reduce the Attack Surface, Secure Critical Applications

- **Wide Coverage:** Apply micro-segmentation policies anywhere your applications run across public, private or hybrid cloud environments.
- **Deep Visibility:** Application-aware visibility, so you fully understand application dependencies before defining micro-segmentation security policies.
- **Intuitive Workflow:** A highly visual workflow and powerful compound rule logic makes creating micro-segmentation policies fast and intuitive.
- **Granular Policies:** Set and enforce process-level rules to tightly control flows between application components, resulting in the strongest security posture

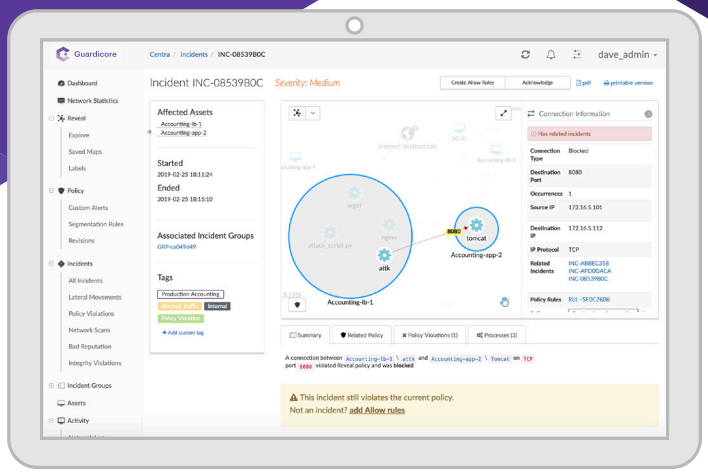
## Micro-Segmentation Simplified

- **Visualize:** Guardicore Centra features best-in-class visibility that automatically discovers and maps all application dependencies and communication flows with process-level context. This visualization, enhanced 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 support 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 of attack.

# Detect More Threats Faster and Respond with Greater Intelligence




Guardicore Centra provides high-fidelity, in-context security incidents, with details on attacker tools and techniques, that help IR teams to prioritize incident investigation and reduce dwell time.




Process-level enforcement detects, alerts, and blocks unauthorized processes from accessing critical application components, reducing the attack surface and limiting lateral movements.

## Beyond Micro-Segmentation: Breach Detection and Response

- **Multiple Detection Methods:** Three detection methods—Dynamic Deception, Reputation Analysis and Policy-Based Detection—form a strong security net to redirect or contain live attacks.
- **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:** Actionable intelligence and recording of attackers' exact tools and methods enable real-time breach response and continuous improvement of micro-segmentation policies.
- **Detailed Forensics:** Incident data is presented in a human-readable fashion alongside evidence, including indicators of compromise, relevant artifacts, and the identifying characteristics of human attackers vs. bots.

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

- **Detect:** Centra features multiple detection methods designed for attacks on cloud and data center infrastructure, including policy-based detection of unsanctioned activity, a high-interaction deception engine that disrupts attackers and captures attack details, and reputation analysis that detects suspicious domain names, IP address and file hashes within traffic flows.
- **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 indicators of compromise to security gateways and security information and event management systems, 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 attacks.

Guardicore

## Comprehensive Protection at Cloud Scale

### Any Environment

Protect workloads in hybrid cloud environments with a combination of on-premises workloads, virtual machines, containers, and cloud instances across Amazon Web Services, Microsoft Azure, and Google Cloud Platform

### Simplify Security

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

### Enterprise Scalability and Performance

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

## Support for the Modern Enterprise IT Infrastructure

**Guardicore Centra is designed to integrate with your infrastructure**

**Memory and System Requirements**
Management Server: 32 GB RAM min, 64 GB RAM recommended, 12 vCPUs, 400GB storage

Deception Server: 32 GB RAM min, 64GB RAM recommended, 8 vCPUs, 100GB storage

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

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

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

**Container Orchestration & Engines**
Docker, Kubernetes, OpenShift

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

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

**Hypervisors**
KVM, XenServer, Microsoft Hyper-V, VMware ESX 5.1 or later for each server

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

## About Guardicore

Guardicore is a data center and cloud security company that protects your organization's core assets using flexible, quickly deployed, and easy to understand microsegmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security—for any application, in any IT environment. For more information, visit **www.guardicore.com**

Guardicore