Guardicore

DATA SHEET

Guardicore Centra™ Security Platform

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

Enterprise IT infrastructure has evolved from traditional data centers to cloud and hybrid cloud architectures with a blend of platforms and application deployment models. This modernization of IT is helping many organizations achieve greater business agility and reduce infrastructure costs. However, it is also creating a larger and more complex security attack surface that does not have a well-defined perimeter. Each individual server, virtual machine, or cloud resource is now a possible point of exposure, and attackers are increasingly adept at moving laterally towards high-value targets once they find a way in.

The Guardicore Centra™ Security Platform is the simplest and most intuitive way to visualize activity in data center and cloud environments, implement precise segmentation policies, protect against external threats, and detect possible breaches quickly.

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. Relevant context is added to this information through a flexible and highly automated labeling process that includes integration with existing data sources like orchestration systems and configuration management databases.

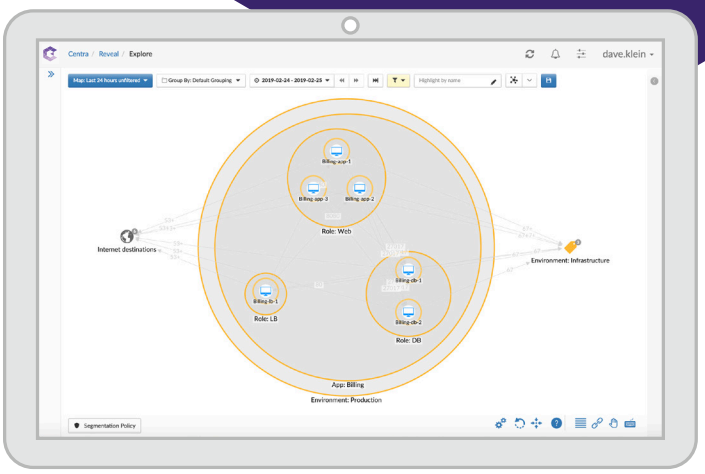
The output is a dynamic map of the entire IT infrastructure that allows security teams to view activity with user- and process-level granularity on a real-time or historical basis. These detailed insights, combined with AI-powered policy workflows, make the creation of segmentation policies fast and intuitive. Centra's segmentation capabilities are complemented by a sophisticated set of threat defense and breach detection capabilities.

Centra is completely decoupled from the underlying infrastructure, so security policies can be created or changed without complex network changes or downtime. In addition, a single set of Centra policies can protect applications across both on-premises data center and public cloud environments.

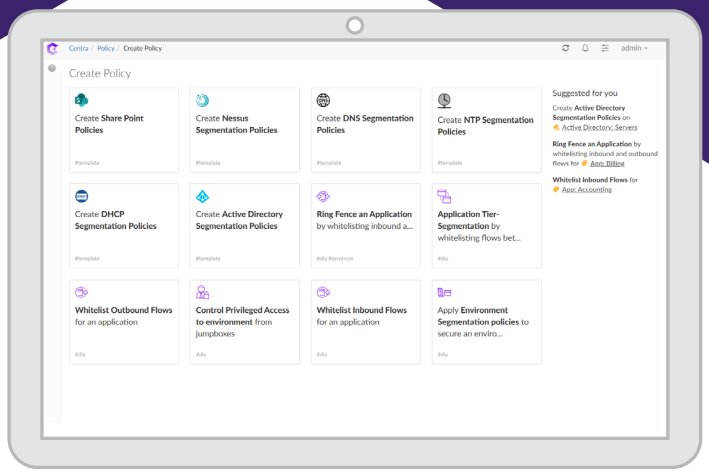
Highlights

- **Real-Time and Historical Visibility**
  Map application dependencies and flows down to the user and process levels on a real-time or historical basis
- **Flexible Asset Labeling**
  Add rich context with a highly customizable labeling hierarchy and integration with orchestration tools and configuration management databases
- **Granular, AI-Powered Segmentation**
  Implement best practice policies in a few clicks using AI recommendations and precise attributes like processes, users, and domain names
- **Broad Platform Support**
  Apply segmentation to an industry-leading selection of modern and legacy operating systems across bare-metal servers, virtual machines, containers, or cloud instances
- **Multiple Protection Methods**
  Augment segmentation with integrated threat defense and breach detection capabilities to reduce incident response time

Simple, AI-Powered Segmentation



Guardicore Centra automatically discovers application dependencies and flows and generates a visual map with custom labels, providing a contextual view of application activity and possible risks.



In the same visual interface, administrators can build segmentation policies quickly based on best-practice templates and AI-powered policy creation workflows.

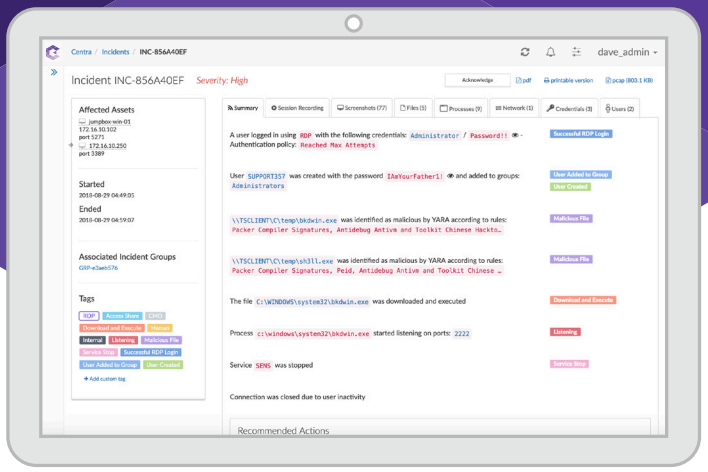
Reduce the Attack Surface, Secure Critical Applications

- **Wide Coverage:** Platform-independent segmentation policies work consistently anywhere your applications run across public, private, or hybrid cloud environments.
- **Deep Visibility:** Application-aware visibility helps you understand application dependencies fully before defining segmentation security policies.
- **Intuitive, AI-Powered Workflows:** A highly visual workflow, best practice policy templates, and powerful compound rule logic make creating segmentation policies fast and intuitive.
- **Granular Policies:** Software-defined policies use attributes like users, processes, and fully qualified domain names to tightly control application flows and reduce the attack surface.

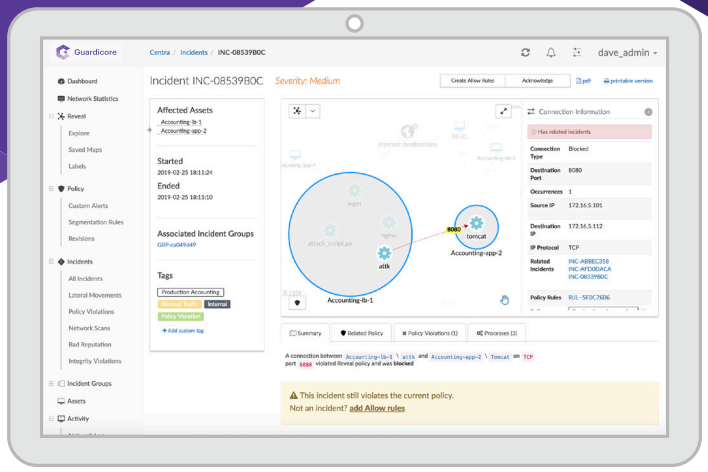
Segmentation Simplified

- **Visualize:** Guardicore Centra's best-in-class visibility automatically discovers and maps all application dependencies and communication flows with process- and user-level context. This visualization, enhanced with automatic orchestration metadata synchronization, enables security teams to label and group all assets and applications quickly and streamline policy development.
- **Build:** Guardicore simplifies segmentation policy development and management. Best practice policy templates and AI-powered workflows make it fast and simple to create highly effective policies. Ongoing visibility into policy effectiveness avoids errors and makes policy refinement easy.
- **Enforce:** Centra's built-in policy enforcement capabilities provide consistent and reliable security regardless of the underlying environment or operating system. 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.

Integrated Breach Detection and Threat Defense



Guardicore Centra provides high-fidelity, context-rich security incidents with details on attacker tools and techniques, helping incident response teams prioritize incident investigation and reduce dwell time.



Process-level and user-level enforcement generates alerts and blocks unauthorized activity, and an integrated threat intelligence firewall stops malware and other external threats from reaching your critical assets.

Beyond Segmentation: Breach Detection and Threat Defense

- **Multiple Detection Methods:** A threat intelligence firewall, reputation analysis, policy-based detection, and dynamic deception form a strong security net to redirect or contain live attacks.
- **Global Intelligence Gathering:** The Guardicore Global Sensor Network, which includes over 10,000 sensors located in data center and cloud environments around the world, streams early threat information to Guardicore Labs for attack identification and analysis.
- **Integrated Response:** Actionable intelligence and recording of attackers' specific tools and methods enable real-time breach response and continuous improvement of 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 includes multiple detection and defense methods to protect cloud and data center infrastructure, including a threat intelligence firewall, reputation analysis that detects suspicious domain names, IP address and file hashes within traffic flows, policy-based detection of unsanctioned activity, and a high-interaction deception engine that disrupts attackers and captures attack details.
- **Investigate:** Centra collects the entire attack footprint, including the files and tools used and the arsenal of weapons that the intruder activates, and performs deep forensics to expose user credentials, attack methods, propagation tactics, and more.
- **Respond:** Centra accelerates 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 violations, and the ability to trigger actions on virtual machines to prevent the spread of damage.

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, Google Cloud Platform, and Oracle Cloud

Simplify Security

Simplify security management with one platform that provides visualization, segmentation, threat defense, and breach detection capabilities

Enterprise Scalability and Performance

Start with focused protection of your most critical digital assets and scale up to protect your full enterprise without complexity, infrastructure changes, or performance bottlenecks

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, 8 vCPUs, 530 GB storage

Deception Server: 32 GB RAM, 8 vCPUs, 100 GB storage

Aggregator: 4 GB RAM, 4 vCPUs, 30 GB storage

Collector: 2 GB RAM, 2 vCPUs, 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 (Vanilla/Mirantis)

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

Hypervisors
KVM, XenServer, Nutanix ESXi and AHV, Microsoft Hyper-V, VMware ESX 5.1 or later for each server

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

Forbes glassdoor #1 Cloud Company to Work For

CRN 100 Coolest Cloud Companies 2020

SC Magazine Best Buy

Info Security Products Guide 2020 Global Excellence Gold

Infosec Awards Winners Cyber Defense Magazine 2020

aws competency

About Guardicore

Guardicore is the segmentation company disrupting the legacy firewall market. Our software-only approach is decoupled from the physical network, providing a faster alternative to firewalls. Built for the agile enterprise, Guardicore offers greater security and visibility in the cloud, data-center and endpoint. For more information, please visit **www.guardicore.com**

Guardicore