SOLUTION BRIEF

Guardicore

Visualize and Secure Hybrid Cloud Applications with Guardicore Centra™

Granular visibility and policy definition for micro-segmentation and governance across data center and cloud workloads

Security and DevOps Are in the Dark

Modern IT infrastructure is increasingly complex to secure. Workloads run on a growing number of technologies, including virtual machines, cloud instances, containers, and bare-metal servers in private, public, and hybrid clouds. Business applications are also evolving from monolithic architectures to distributed models, increasing the number of processes running in the data center.

As a result, security teams are challenged to secure increasingly dynamic environments, maintain visibility into running applications, monitor and enforce compliance. When deploying or modifying security policies, security teams are often in the dark. Because they cannot see the actual application flows in their environments, change processes are slowed and security policies are rendered ineffective. And when sophisticated attackers do get in, traditional security tools and policies fail to detect their movements, allowing them to dwell inside the data center for months.

Guardicore Centra for Visualization, Micro-Segmentation, and Breach Detection

Guardicore Centra combines process-level visibility into applications and workloads with granular policy definition, enabling security teams to discover, visualize, control, and monitor activity across data center and cloud environments. By better understanding applications and interdependencies, organizations can proactively implement more granular policy controls and detect breaches faster.

Once installed, Guardicore Centra automatically generates a detailed visual map of activity across all environments in use. Process-level activity is correlated with network events, giving administrators a visual view of all workloads. Administrators can drill down for more detail, including specific assets, processes and time frames, to gain a full understanding of communications within and between data center and cloud environments. Guardicore Centra also makes creating application-centric micro-segmentation policies simple, fast, and non-disruptive.

Highlights

- **Process-Level Visibility**
  Visualize all applications and their traffic, including process-to-process communications.
- **Micro-Segmentation**
  Define and manage granular, application-aware micro-segmentation policies based on visual representations of infrastructure and activity.
- **Contextual Relevance**
  View application activity and define security policies in relevant ways through integration with orchestration tools and sophisticated nested grouping options.
- **Real-Time and Historical Views**
  View visualizations on both a real-time and historical basis and create multi-tier views that make understanding complex enterprise workflows and creating sophisticated compound rules easy.
- **Breach Detection**
  Detect attacks by identifying suspicious activity between applications and processes.
- **Compliance**
  Monitor infrastructure-wide communications against defined policies and generate incidents for any variations.

Guardicore Centra simplifies micro-segmentation with a five-step process

▶ **Step 1.**
Discover and map your application dependencies. This simplified discovery approach helps identify which assets should be grouped into micro-segments and prioritize policy decisions based on workload roles, relationships, and vulnerabilities.

▶ **Step 2.**
Label and group your assets based on functions and business context. Once assets are defined and grouped, you can easily create separation policies for the different groups, including dynamic labels that extend policies to auto-scaling applications.

▶ **Step 3.**
Define micro-segmentation policies. Automatically suggested rules simplify the creation of segmentation policies for individual or groups of assets update dynamically as applications are added or removed.

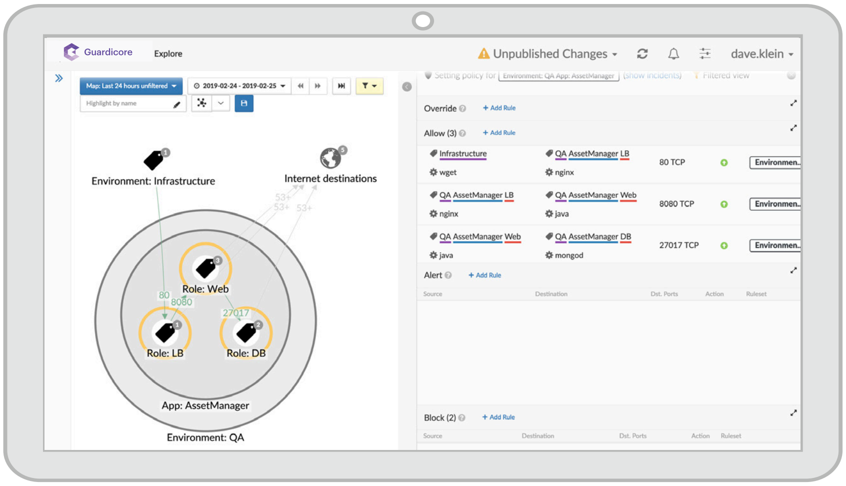
▶ **Step 4.**
Monitor and refine micro-segmentation policies. Set initial policy actions to alert security administrators of non-compliant traffic flows and unauthorized processes. Diagnosing alerts will help optimize micro- segmentation policies to ensure they won't block legitimate traffic.

▶ **Step 5.**
Enforce micro-segmentation policies. Quickly and easily convert your high-confidence rules from alerting to blocking mode to actively prevent policy violations.

Guardicore

Micro-Segmentation

Implement Application-Aware Micro-Segmentation Policies—Guardicore Centra makes it simple to develop and deploy granular security, data compliance, and governance controls from the data center to the cloud without disrupting business performance.



Source	Destination	Dst. Ports	Action	Ruleset
Infrastructure wget	QA AssetManager LB nginx	80 TCP	●	Environmen..
QA AssetManager LB nginx	QA AssetManager Web java	8080 TCP	●	Environmen..
QA AssetManager Web java	QA AssetManager DB mongod	27017 TCP	●	Environmen..

Guardicore Centra provides complete process-to-process visibility and segmentation policy management that spans all on-premises and cloud environments and all application delivery models.

Breach Detection

Guardicore Centra enables security teams to define granular security policies between applications and monitors those policies for variations and suspicious activity. Variations from defined policies are presented in the detailed visual map and logged as real-time security incidents within the incident view of the Guardicore Centra management console for further investigation.

Protect Applications—Protect specific applications running in your on-premises and cloud infrastructure. Guardicore Centra monitors new connections to processes or assets, alerting in real-time on unknown or unauthorized connections.

Detect Breaches—Detect malicious processes that are using trusted assets and following security policies to communicate with other applications. Guardicore Centra analyzes the reputation of file names, domain names and IP addresses to investigate suspicious connections.

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.

More information is available at www.guardicore.com

v. 3.0