

Visualizing and Securing Data Center Applications with GuardiCore Reveal™

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

Security and DevOps Are in the Dark

Modern data centers are becoming increasingly complex to secure and maintain. Workloads are running on a growing number of technologies, including virtual machines, containers, and bare-metal servers in private, public and hybrid clouds. Business applications are moving from monolithic models to distributed, scalable ones, increasing the number of processes running in the data center.

As a result, security teams are challenged to secure increasingly dynamic data centers, maintain visibility into running applications, monitor for compliance and quickly detect breaches. When modifying or deploying new security policies, security teams are often in the dark - they cannot see the actual application flows in their data center - leading to slow change processes and inadequate security policies. 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 Reveal for Visualization, Breach Detection and Segmentation Policy Management

GuardiCore Reveal, a key component of the GuardiCore Centra™ Security Platform, provides process-level visibility into applications and workloads combined with granular policy definition enabling security teams to discover, visualize, control and monitor activity inside the data center. Teams gain a better understanding of applications and can detect breaches faster by identifying suspicious behavior.

Once installed, GuardiCore Reveal automatically generates a comprehensive visual map of all activity inside the data center, correlating process-level activity with network events, allowing administrators to get a quick and visual view of all workloads. Administrators can drill down on more details, such as specific assets, processes and time frames, to ensure a full understanding of communications inside the data center. GuardiCore Reveal also provides a practical means of creating and deploying application-centric microsegmentation policies quickly without disrupting data center operations.



Highlights

- Process-level Visibility
 Visualize all applications and
 their traffic, including process to-process communications.
- Time-Based View
 Visualization and usage
 reports are based on actual
 traffic monitored and can be
 viewed in different timeframes,
 including historical information.
- Breach Detection
 Detect attacks by identifying suspicious activity between applications and processes.
- Micro-Segmentation
 Define and manage granular, application-aware microsegmentation security policies down to the process level.
- Compliance
 Monitor all data center
 communications against
 defined policies and generate
 incidents for any variation.



GuardiCore Reveal simplifies micro-segmentation and minimizes disruption with a five-step process

Step 1. Discover, visualize, and map your network application process communication flows. 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 rules and separation policies for the different groups, including dynamic labels which extend policies to auto-scaling applications.

Step 3. Define microsegmentation policies.

Automatically suggested policy rules simplify the creation of segmentation policies for individual or groups of assets, which can be dynamically updated quickly and easily when applications are added or removed.

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

Step 5. Enforce microsegmentation policies.

block legitimate traffic.

Quickly enforce against policy violations through tight integration with your existing security tools.

Breach Detection

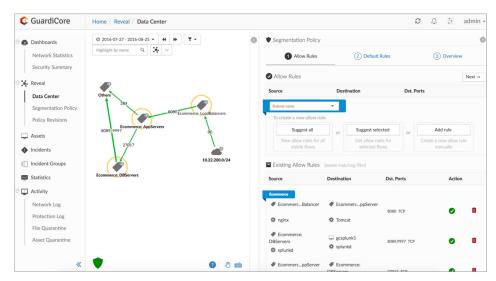
GuardiCore Reveal enables security teams to define granular security policies between applications and monitors those policies for variations and suspicious activity. Variations from defined policies are presented in the comprehensive visual map, and logged as real-time security incidents within the Incident View of the GuardiCore Centra management console for further investigation.

Protect Applications – Protect specific applications running in the data center. GuardiCore Reveal 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 Reveal analyzes the reputation of file names, domain names and IP addresses to investigate suspicious connections.

Micro-Segmentation

Implement Application-Aware Micro-Segmentation Policies – GuardiCore Reveal simplifies the process of developing and deploying granular security, data compliance and governance controls inside the data center without impacting business performance.



GuardiCore Reveal provides complete process-to-process visibility and segmentation policy management for the entire data center, across multiple VMs and between assets (public or private).

About GuardiCore

GuardiCore is a leader in Internal Data Center Security and Breach Detection. Developed by the top cyber security experts in their field, GuardiCore is changing the way organizations are fighting cyber attacks in their data centers.

More information is available at www.guardicore.com