Guardicore

SOLUTION BRIEF

Discover, Map and Visualize Hybrid Cloud Applications with Guardicore Centra™

Application discovery mapping with deep visibility for cloud migration, micro-segmentation and governance across hybrid data center and cloud workload environments

Security and DevOps Are in the Dark

Modern IT infrastructure is increasingly complex to understand and visualize. Infrastructure is deployed using a growing number of workloads based on multiple 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 sub-components and processes running in the data center. As a result, when there's a need to migrate applications to a new environment, modernize or secure it, DevOps teams are challenged to identify dynamic environments, maintain visibility into running applications, and 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. During application migration, some elements are either left behind, broken or worse - enable sophisticated attackers to bypass the traditional security controls and dwell inside the data center for weeks and 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. The same tool used for visualization of end-to-end application dependencies is used for fast cloud migration. By Better understanding applications and interdependencies, organizations can proactively identify how applications are communicating and then use this information for migration, 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.
- **Contextual Relevance**
  View application activity and define security policies in relevant ways, through integration with orchestration tools and sophisticated nested grouping options.
- **Application Dependency Mapping**
  View how application components are dependent and communicate with each other across any environment, down to process level and the interflow communications it generates.
- **Real-Time and Historical Views**
  View visualizations on both real-time and historical basis and create multi-tier views that make understanding complex enterprise workflows and creating sophisticated rules easy.

Security Capabilities

- **Micro-Segmentation**
  Define and manage granular, application-aware micro-segmentation policies based on visual representations of infrastructure and activity.
- **Breach Detection**
  Detect attacks by identifying suspicious activity between applications and processes.