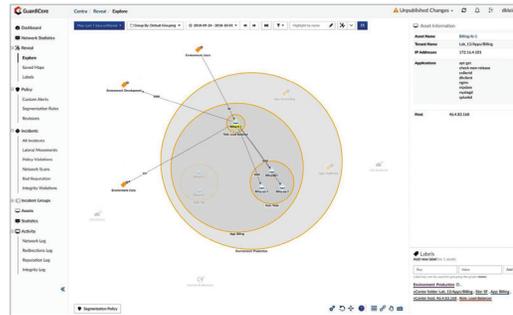




Virtualization and cloud-based security

Guardicore



DETAILS

Vendor Guardicore, guardicore.com

Flagship Product: Centra Security Platform

Price: Annual subscription based on the type and quantities of servers. Entry level customers start at \$25,000 per year.

Innovation: Delivering a solution that truly simplifies the management and enforcement of micro segmented networks.

Greatest Strength: A company so passionate about improving security that it extends beyond the commercial platform and contributes to the cybersecurity eco system with no cost offerings like Infection Monkey.

Successfully exfiltrating data from enterprise environments requires access to the network and traversing resources to locate the desired data sources. Traditional firewalls, intrusion prevention systems and other network-based security systems are designed to inspect and secure traffic moving into the environment. Most modern network environments now support microsegmentation, which gives organizations greater control over the growing amount of the lateral communication between servers, bypassing perimeter-focused security tools. The granular nature of this technology limits the potential impact of a hacker accessing an environment, but dramatically increases the complexity of managing access rights.

Guardicore focused on protecting servers, which is a purposeful departure from the more common focus on endpoint and perimeter security. The company simplified policy management for environments where microsegmentation is used to limit lateral network traffic among servers. The Centra Security Platform is comprised of an integrated solution set that includes visualization, microsegmentation, detection and response.

Visualization analyzes network topology

collecting and indexing the details for easy retrieval. User queries can be answered with text-based responses or interpreted through the visual graphic interface. The resulting “map” that is developed serves as the foundation for identifying segmentation and detection requirements.

A centralized policy that is distributed and enforced throughout the network. Policy feedback is provided by agents installed on the servers and used for validating traffic patterns. This approach overcomes the shortcomings of traditional segmentation and provides high levels of granularity and control through a single easy-to-use interface.

Data collected by agents are also used to support the detection and response capabilities. A high-resolution view of network behavior is evaluated against third-party threat and reputation data to identify malicious behavior. As bad behavior is identified, the policies can activate blocking at the network and device levels. From legacy systems to the latest developments in container-based applications, Guardicore provides visibility across the enterprise network, which reduces risk while enhancing compliance.

— Rob Cote, program director, SC Lab



Guardicore

Levinstein Tower, 23rd floor
23 Menachem Begin Road, Tel Aviv 6618356
info@guardicore.com
www.guardicore.com