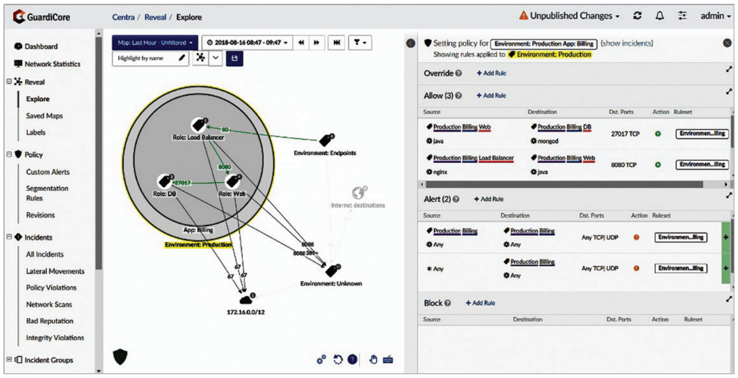
Guardicore

Centra Security Platform



Setting policy for Environment: Production App: Billing (show incidents)
Showing rules applied to Environment: Production

Allow (3)

Source	Destination	Dst. Ports	Action	Ruleset
Production Billing Web java	Production Billing DB mongod	27017 TCP	●	Environmen...lling
Production Billing Load Balancer nginx	Production Billing Web java	8080 TCP	●	Environmen...lling

Alert (2)

Source	Destination	Dst. Ports	Action	Ruleset
Production Billing Any	Production Billing Any	Any TCP| UDP	●	Environmen...lling
Any	Production Billing Any	Any TCP| UDP	●	Environmen...lling

Block

Source	Destination	Dst. Ports	Action	Ruleset

Guardicore's Centra architecture is based on three tiers. Collectors are deployed at the infrastructure level while agents are deployed at the guest level. An optional aggregation tier is installed only when agents are deployed, and centralized management and deception is usually provided as SaaS but can also be deployed on-premises.

Native enforcement has Layer 4 and 7 controls, no reliance on firewalls, and consistency across operating systems. It comes DevOps-ready with agent and agentless options. Competitive advantages include visibility, micro-segmentation, breach detection and deception. Layer 7 visibility offers rich context. Automatic application and common services discovery, flexible labeling, automated policy recommendations and Layer 4 and 7 enforcement for all platforms are part of Guardicore's microsegmentation. Breach detection encompasses multiple techniques, including reputation services and file integrity monitoring. Deception is distributed and dynamic with high-interaction, full platform integration and lateral movement focus.

Guardicore Reveal provides infrastructure maps on service interaction and application location. Application Discovery works across clouds and shows different environments. This highlights application data sources, utilized ports and data destinations.

Maps can show past information to analyze a specified time period and all communications occurring down to individual server or process levels. Microsegmentation puts policies onto servers and is Guardicore's most important offering in our opinion. They push policies to servers. On existing servers and IP addresses, regardless of environment, you can enforce policies across all datacenters and clouds with agents like a massive distributed enforcement layer controlled from one centralized point. Users choose between whitelist and blacklist models, or some combination of the two.

Guardicore makes centralizing policies quick and easy with the ability to write global security rules. You can block ports from a single point. To prevent VM machines from communicating, just create the policies. This extreme flexibility even allows blocking non-PCI-compliant machine traffic from communicating with PCI-compliant machines.

When a server tries performing lateral movements, failed connections are tracked and permitted. Attackers' attempts are redirected in real time to connect to their deception engine. This presents a Windows or Linux machine for the attacker to attack instead. When they try connecting to another machine, they are redirected to one belonging to Guardicore. As soon as malicious behavior is confirmed, a real-time alert is sent to the user.

— Katelyn Dunn
Tested by Matthew Hreben

DETAILS

Vendor Guardicore

Price Guardicore Centra is priced based on an annual subscription. Pricing starts at $25,000 per year and subscription price is based on number of protected assets.

Contact guardicore.com

Features	★★★★★
Documentation	★★★★★
Value for money	★★★★½
Performance	★★★★★
Support	★★★★★
Ease of use	★★★★★

OVERALL RATING ★★★★★

Strengths Centra's container support gives you the ability to dive into details all the way to the process level on public and private clouds.

Weaknesses None that we found.

Verdict Combining the scalability from small to large enterprise environments with the ability to group virtually all types of environments together is incredibly useful. Having the choice to utilize agents or the agentless approach for deployment options gives a nice blend of customizability.

Guardicore

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

Reprinted from SCMagazine.com, February 2019 • www.scmagazine.com