

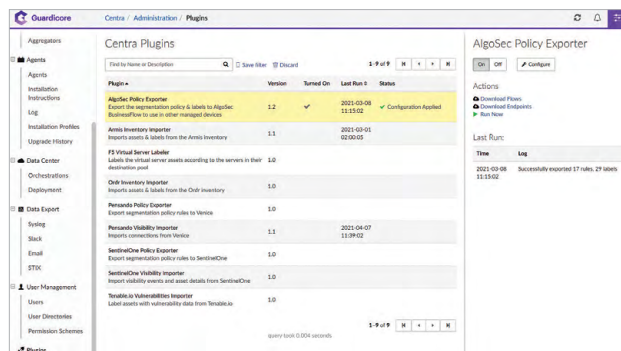


Partner solution brief

AlgoSec and Akamai, stronger together

Akamai Guardicore Segmentation is a security platform that creates human-readable views of your compute infrastructure. It extends security analytics and policy to multi-cloud apps by using behavior and attribute-driven micro-segmentation policy generation and enforcement. It reduces complexity by working consistently across any environment, reduces risk by enabling granular micro-segmentation policies, and enables innovation by integrating security into the DevOps and IT automation workflows without requiring application changes.

Guardicore Segmentation offers complete workload protection over users and endpoints, networks, including network ADCs, and application workloads, both on-premises and in the cloud. However, relying on Guardicore Segmentation alone does not enable infrastructure policy enforcement over your firewalls, SDN and cloud security controls.









Enforcing micro-segmentation throughout your entire network

Organizations need consistent segmentation policies, across application workloads and infrastructure. Guardicore Segmentation enforces micro-segmentation policies over your workloads but not on the rest of your network. AlgoSec extends the segmentation policy originating from Guardicore Segmentation to the rest of your network – cloud, SDN and on-premises technologies.



Why integrate Akamai with AlgoSec?

-  Streamlined and consistent network security policy management across your entire hybrid network environment.
-  Visibility into all network security policies across your entire hybrid network environment.
-  Extend implementation of micro-segmentation projects to legacy and appliance-based environments, as well as hybrid networks across the on-premises and public cloud environment.
-  Ensure consistency of segmentation policies and labeling, while avoiding duplication, across your entire network.
-  Optimize and present Akamai-enforced policies to non-technical business application owners
-  Make changes and secure your entire network environment within minutes.

Effectively managing risk, vulnerabilities, and compliance

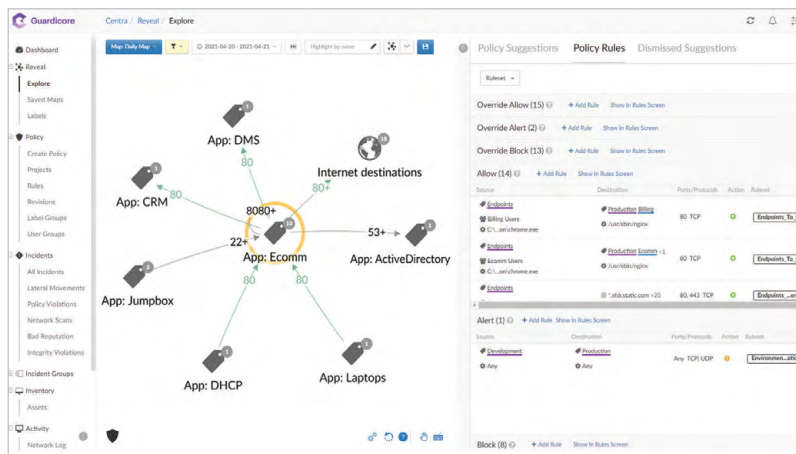
A micro-segmentation project cannot be successful without managing risk, vulnerabilities, and compliance in the context of affected business applications. A successful micro-segmentation strategy requires a clear understanding of what business applications map to which security rules.

By integrating Guardicore Segmentation with AlgoSec, the AlgoSec AppViz addon discovers, identifies, and maps business applications, ensuring visibility of the network connectivity flows associated with each business application. This provides critical information regarding the firewalls and firewall rules supporting each connectivity flow.

It is important to understand what business applications are impacted when evaluating the risk and compliance state of an organization's network segmentation policy. With AlgoSec, you can prioritize vulnerability and patches based on the affected applications. You can view aggregated information about the network security risks and vulnerabilities relevant to each business application.

AlgoSec's AppViz provides a concise, human-readable view into business application connectivity, including:

- Automated application architecture
- Security governance zone overlay and diagram
- Optimized business application flows
- Automated mapping of business applications to downstream device changes



About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to secure application connectivity by automating connectivity flows and security policy, anywhere.

The AlgoSec platform enables the world's most complex organizations to gain visibility, reduce risk, achieve compliance at the application-level and process changes at zero-touch across the hybrid network.

Over 1,800 of the world's leading organizations trust AlgoSec to help secure their most critical workloads across public cloud, private cloud, containers, and on-premises networks.

