

Versatility in Security Policy and Operations

As the adoption of cloud infrastructure and containers increases, the value of traditional perimeter-focused security wanes, yielding to a growing need for visibility into lateral movement among data center and cloud assets. Zero Trust network segmentation and its inherent granularity offer several benefits in this scenario. As a Network and Security Engineer at the small tech company CS-Novidy put it, Guardicore's deception features provide a rich telemetry of lured origins and are a "great resource for any active defense strategy."

Prevent Lateral Movement

Zero Trust network segmentation isolates workloads and reduces attack surfaces, making it more difficult for attackers to move laterally across networks. A Senior Network Security Engineer at a tech services company with over 50 employees spoke to this issue when he explained that Guardicore provides visibility of the entire data center and helps stop lateral movement of attacks.

A Network & Security Engineering Manager at Teleflora, a retailer with over 500 employees, uses the tool to segregate the company's various environments: staging, production, QA, and applications. He said, "We are essentially replacing our traditional, internal firewalls and depending completely on Guardicore to secure all of our applications."

"..Guardicore provides visibility of the entire data center and helps stop lateral movement of attacks."

[Read review »](#)