ILLUSIVE PLATFORM FEATURE BRIEF:

Illusive Distributed Management

The Illusive Distributed Management solution allows Illusive customers with segregated environments (including subnetworks with limited connectivity between them) the freedom to deploy a single management server in a centralized location and deploy lightweight connectors in each segregated zone. This will allow the coverage of the entire environment with one Illusive system and with a limited number of connections between the zones and the management server. As a result, organizations do not need to go against their network security best practices by weakening firewalls, nor do they need to deploy and manage several completely separated Illusive systems.

BENEFITS

- Have a single pane of glass for the SOC and SecOps teams to manage Illusive across their entire environment
- Minimize security risks, as there is no need to change security policies or need to poke holes in the firewall
- Reduce CAPEX by replacing secure zone management servers with VM, Linux-based connectors, eliminating extra Windows licenses
- Cloud-friendly network management, enabling security teams to more easily defend hybrid ecosystems

Strengthen security with reduced risk

Increase SOC and SecOps efficiency

Leverage the advantages of the Illusive platform—network visibility, deception-based threat detection and attack intelligence—across dynamic ecosystems, but without sacrificing security protocols.

Illusive Distributed Management eliminates the need for SOC teams to manage multiple, separated Illusive systems. Deceptions, forensics and other capabilities are easily manageable, covering an entire network environment.

How Illusive Distributed Management Works

1. Centralized management is in place as a single pane of glass
2. Each segmented zone is deployed with one or more Illusive connectors
3. Each connector establishes a secure tunnel to the management server
4. Illusive data analysis, deceptions planting and forensics collection are cover all zones