DxOdyssey vs. VPNs

DxOdyssey and VPNs both allow connections to and from workloads that can reside on premises or in the cloud. This document details the differences in features of the two in terms of management, high availability, security and more.

	DxO	VPNs	Why It Matters
Hardware Requirements	Flexible. Any commodity OS/ container running Windows or Linux, on any hardware, in any mix	Rigid. Proprietary VPN router appliances required	A software-based approach gives organizations the flexibility to decide which platform to deploy on
Ease of scalability	Simple: Add resources to the existing gateway to scale up, or add another gateway to scale out	Moderate: replace existing gear to scale up	
High Availability / Resiliency	Yes. Gateways can be scaled out for load balancing and HA. If a gateway goes down, another in the group will automatically resume the connection	None. If the VPN goes down, the connection is lost until the hardware is updated or replaced	
Cost for Cloud Connection	No additional cost	Yes, requires paying a cloud vendor an hourly fee for connection	
Security	Users get access to specified applications resulting in little to no network attack surface	Users get access to the entire network, creating a very large network attack surface	Reducing vulnerabilities and having no open ports allows a secure perimeter and fewer opportunities for bad actors to attack
Configuration & Maintenance	Install and connect, no appliances to configure or maintain	Create and manage firewall rules, access control lists, etc.	