DxOdyssey vs Other SDP Solutions

DxOdyssey and other SDPs both allow the secure access of resources whether they're on-premises or in the cloud. This document details the differences in features of the two in terms of the data transmission protocol, high availability, integrations and more.

	DxO	SDP Solutions	Why It Matters
Data Transmission Protocol	UDP / DTLS	TCP / TLS	UDP is more performant due to lower latency and is more secure because the data packets are segmented. DxO also implements some TCP RFCs to make it reliable.
Controller Node Requirement	No. DxOdyssey gateways join with one another via a cloud matchmaking service, and then communicate directly.	Yes. Intrusive middleman must authenticate every connection, or, in some cases, data actually passes through the controller.	A lightweight "matchmaking service" is less intrusive and does not become a bottleneck once the gateways are introduced, resultingin better security and performance.
True Failover Clustered HA Gateways	Yes. If a gateway goes down, another in the group will automatically resume the connection.	Not true clustering. Some have very rudimentray HA with significant caveats	High availability ensures that data is readily available in case of disasters and downtime.
DNS Dependency for Gateways	No	Yes	Gateways that require DNS for resolution increase complexity and can also reduce security by requiring open ports for gateway communication.
Integrations	Yes, open API with simple integration points.	Yes, limited.	DxOdyssey can integrate with other authentication or management tools very easily. Other SDP vendors have API capabilities, but are much more limited in what they can connect with.
Adherence to Cloud Security Alliance SDP Specification	No	Yes	DH2i staff are members of the CSA SDP Working Group, but DxOdyssey does not strictly adhere to the specification. We believe that our proprietary approach adds more value over the spec.