

# COMPETITIVE ADVANTAGE

## GOING WAY BEYOND SD-WAN

## Dispersive™ Virtual Network

Dispersive is changing the networking paradigm. Standard approaches to networking all have one crucial flaw in common: they all use a single path to transfer data. To avoid this single point of compromise and congestion, the Dispersive™ Virtual Network (DVN) does things differently.

Dispersive™ Virtual Network separates the network and management control planes similar to SDN, and allows full programmability of the network applications and services.

The Dispersive™ Virtual Network solution provides ultra-secure networks authenticating and encrypting network traffic simultaneously over multiple paths.

The multiple paths, which are dynamically routed through deflect waypoints, provide a highly secure overlay network, and inherently enable dynamic resiliency.

This improved security and resiliency, when coupled with traditional SDN benefits of flexibility and high performance, make it a differentiated alternative to traditional offerings.

Feature	VPN	SD-WAN	DVN	Dispersive Advantage
Centralized Network Control and Policy Management	🟡	🟢	🟢	
Rate Limiting Control	✖	🟢	🟢	
Rate Smoothing (Voice/Video)	✖	🟢	🟢	
Resiliency	✖	🟡	🟢	Constant multi-path rolling enables superior response to failure conditions
Bandwidth Aggregation and Scalability	✖	🟡	🟢	Multi-NIC leverages all available network interfaces
Dynamic Path Switching	✖	🟡	🟢	Channel rolling and paths selection inherently efficient with DVN core architectural design
Per Packet Load Balancing	✖	🟡	🟢	Balancing of packets on multiple paths based on individual channel/path performance
Data/Control Plane Encryption	🟡	🟡	🟢	Multi-layers encryption and obfuscation on paths, channels and segments
Service Micro-Segmentation	✖	✖	🟢	Dispersive™ Virtual Network secures and segments individual application services while adding multiple layers of encryption on data in motion on separate paths, channels and segments
Diverse Network Routing	✖	🟡	🟢	
Dynamically-Routed Encrypted Paths	✖	✖	🟢	
Endpoint Authentication	🟡	✖	🟢	Authentication while maintaining end-point non-attribution. DVN performs network mapping as a primary step during the discovery phase of an attack.
Enhanced Security (Obscure Endpoints, Cyber Attack Surface Reduction, DOS/DDOS Mitigation, etc.)	✖	✖	🟢	Reduces attack surface and eliminates common VPN vulnerabilities
Common Edge Software Across IoT, Mobile Workforce, Cloud, uCPE	✖	✖	🟢	
Performance Improvements (Up to 10X Over IPSEC Tunnels)	✖	✖	🟢	

KEY: 🟡 AVERAGE    🟢 EXCELLENT