DATA SHEET

COMPARISON:

Data Aggregation Technologies

Network owners are struggling with managing the terabytes of device-generated data and status reports. Aggregating data is an emerging approach that enables cyber threat hunting, network performance analyzing, and other functions so essential for maintaining the integrity of large, complex data ecosystems. Aggregating data with an appliance that delivers a hardware-based security guarantee is best practice.

The table below summarizes the functionality and relative strengths and weaknesses of three distinct technological approaches to data aggregation: network taps, network packet brokers, and XD Matrix, a new hardware-based data aggregation solution from Owl Cyber Defense.

	NETWORK PACKET BROKERS	NETWORK TAPS	XD MATRIX
FUNCTIONS	1. Collects and aggregates network traffic on behalf of security, analytics, and performance monitoring tools. 2. Filters network traffic, so each network device receives exactly what it needs and no more (e.g., application filtering) 3. Offloads services such as decryption, so tools can perform their primary tasks more efficiently.	1. Duplicates and redirects packets.	1. Aggregates 8-32 discrete flows and delivers them via 2-8 output ports. 2. Enforces one-way transfer in a hardware-enforced data pipeline. No chance of data back-flow.
STRENGTHS	Powerful, multi-purpose network devices that enhance network performance in numerous ways, including: 1. Increases the resiliency and security of networks and security tools by balancing workloads and eliminating single points of failure (i.e., bypass and load balancing).	Simple, single-purpose network devices intended to copy and redirect network traffic to predefined network locations. 1. Little to no performance degradation. Generally maintains line rate and introduces absolutely minimal latency. 2. Generally low cost devices. 3. Generally require little to no maintenance, configuration, or patching overhead. Low life-cycle costs.	Powerful, cybersecurity-focused appliances. The appliance's security guarantees, including network whitelisting, packet filtering, protocol breaks, and one-way flow enforcement executed entirely in FPGA hardware. 1. The data paths are invulnerable to the ecosystem of x86/Windows exploits. Bad actors would have to develop custom tools and gain access to the appliance itself to perform any exploit. 2. Minimal configuration or firmware updates required for the FPGA-enforced data paths. Low maintenance overhead and low lifecycle cost. 3. The management plane/Administrative Processor is secured by Owl's Trusted Operating System - the same OS used by Owl's cross-domain solutions.
WEAKNESSES	Not purpose built to only deliver traffic via hardware-enforced flow control and packet filtering to network security and monitoring tools (i.e., DCO, CSfC CM) 1. Most or all network traffic must pass through a NPB. The Packet Broker itself is a potential single-point-of-failure. 2. Potential for mixing traffic that should not be mixed. Security concerns. 3. Expensive and challenging to configure. Needs regular updates. 4. No way to reliably enforce one-way data transfer (OWT) to security monitoring nodes. No data diodes or hardware flow enforcement. 5. CPU-based security guarantee using a commercial operating system. Vulnerable to all of the tools and techniques developed by hackers to exploit the x86/Windows/Linux ecosystem.	Not purpose built for cybersecurity. Will generally copy and forward all data, including malware, that may be embedded in data packets. Taps are not cybersecurity devices. 1. They don't generally perform a protocol break (e.g., digital-to-light-to-digital) as part of the overall One-Way Flow Enforcement. Degrades the overall security guarantee. 2. Little or no packet filtering capability. No malware protection capability. 3. Some taps claim to have data diode features. Few offer details about the actual DD hardware. Far fewer still have ever offered their DD features for security evaluation and certification. 4. May require multiple taps to achieve adequate data aggregation.	XD Matrix is not a multi-purpose device that enhances overall network performance; it is not a network packet broker. Neither is XD Matrix a simple data tap - it is far more capable. 1. Not as inexpensive as network taps. 2. Not as multi-capable as Packet Brokers.