T E C H N I C A L W H I T E P A P E R

SDVN-Powered Storage

How Software Defined Virtual Networking Powered DASSET Platform as Sovereign Data Infrastructure

Your DATA | Your ASSET | Your AI

PlanetX Labs
www.planetxlabs.io
Confidential | March 2026

Table of Contents

1. Executive Summary 4
2. The Problem: Data Without Sovereignty 5
2.1 Fragmented Ownership 5
2.2 Security Without Sovereignty 5
2.3 Intelligence Requires Exposure 5
2.4 Storage Has Stalled 5
2.5 Networking: The Missing Layer 5
3. The DASSET Platform: Three Pillars of Innovation 6
3.1 Secure Data Foundation (SDVN) 6
3.2 Intelligent Storage 6
3.3 Private Intelligence Layer 6
4. SDVN: The Networking Foundation 7
4.1 Architectural Overview 7
4.2 Core Technical Capabilities 7
5. How SDVN Powers the DASSET Storage Platform 9
5.1 Every Storage Node Becomes a Secure Network Node 9
5.2 Encrypted Peer-to-Peer Data Replication 9
5.3 Network Slicing for Data Governance 10
5.4 AI-Aware Traffic Prioritization 10
5.5 Sovereign Mesh Clustering 10
6. Security Architecture 11
6.1 Zero-Trust Access Model 11
6.2 Multi-Layer Encryption 11
6.3 Continuous Trust Evaluation 11
6.4 Full Lifecycle Audit Logging 12
6.5 Explicit Threat Model and Security Guarantees 12
6.6 Privacy as Architecture 12
6.7 Cryptographic Design Principles 13
7. SDVN vs. Traditional Approaches 14
7.1 Structural Data Sovereignty 14
7.2 Four-Layer Defensibility 14
8. Deployment and Partner Integration 16
8.1 Client SDK 16

8.2 Hosting Model 16
8.3 Federation Model 16
8.4 Proven at Enterprise Scale 16
9. The DASSET Product Portfolio 17
10. Strategic Positioning 18
11. Conclusion 18
Contact 19

1. Executive Summary

The convergence of AI proliferation, accelerating data growth, and heightening privacy regulations has created an urgent need for a new class of data infrastructure—one that places ownership, intelligence, and security directly in the hands of users rather than centralized cloud providers.

DASSET, developed by PlanetX Labs and powered by SDVN (Software Defined Virtual Network), transforms storage into sovereign data infrastructure. Every device becomes simultaneously:

- A secure network node
- A private AI compute engine
- A self-governing encrypted data vault

Accessible globally—without VPNs, port forwarding, cloud relay servers, or third-party intermediaries.

Unlike traditional storage products that secure files at rest but depend on fragile networking overlays, DASSET embeds identity, encryption, routing intelligence, and segmentation directly into the storage fabric. This white paper details how SDVN powered DASSET storage product as a sovereign edge infrastructure platform.

2. The Problem: Data Without Sovereignty

Today's data landscape is defined by a fundamental paradox: data exists everywhere, yet users control almost none of it. Five interconnected challenges define this crisis.

2.1 Fragmented Ownership

Personal and business data is scattered across cloud platforms, local devices, SaaS applications, and social media ecosystems. There is no unified control plane that lets an individual or organization manage retention policies, access permissions, and data lifecycle across all of these surfaces. Each platform imposes its own governance model, creating silos that resist interoperability.

2.2 Security Without Sovereignty

Cloud providers invest heavily in infrastructure security, but this protects the platform—not the user's autonomy. Users surrender governance over data retention, visibility into how their data is processed, and meaningful control over who can access it. The provider, not the owner, determines the rules.

2.3 Intelligence Requires Exposure

AI services increasingly require uploading sensitive data into centralized ecosystems for processing. Whether using generative AI models, analytics platforms, or machine learning pipelines, the current paradigm demands that users hand over their most sensitive information to benefit from intelligence. This creates an unacceptable trade-off between capability and privacy.

2.4 Storage Has Stalled

Traditional NAS (Network Attached Storage) and DAS (Direct Attached Storage) protect files at rest, but they cannot protect identity, context, or support future AI workflows. These systems were designed for an era of static file serving. They lack the networking intelligence, encryption architecture, and compute capabilities required for the AI-driven, globally distributed data environments of today.

2.5 Networking: The Missing Layer

Even when organizations deploy on-premises storage, they face a networking gap. Accessing devices remotely requires VPN configurations, DDNS services, port forwarding, or cloud relay servers—each introducing complexity, security vulnerabilities, and performance compromises. Traditional networking was not designed for user-owned, globally accessible, identity-verified data infrastructure.

3. The DASSET Platform: Three Pillars of Innovation

PlanetX Labs addresses these challenges through DASSET, a platform built on three integrated pillars that together rebuild how data moves, lives, and thinks.

3.1 Secure Data Foundation (SDVN)

The networking substrate that provides zero-trust connectivity, end-to-end encryption, global access without VPN or relay infrastructure, and a user-owned access model. SDVN is not an add-on; it is the foundational layer upon which all DASSET capabilities are built.

3.2 Intelligent Storage

A universal operating system that runs across diverse hardware platforms, delivering automated backup and lifecycle management, a unified data graph across all connected devices, and a native AI-supported file system. This layer transforms raw storage into an intelligent data platform.

3.3 Private Intelligence Layer

Local AI inference powered by on-device compute, accessed through a natural language interface with adaptive compute orchestration. Intelligence runs where the data lives—at the edge—eliminating the need to expose sensitive information to cloud AI services.

4. SDVN: The Networking Foundation

SDVN (Software Defined Virtual Network) is a programmable, encrypted overlay network that creates on-demand private networks of SDVN nodes on top of existing Internet infrastructure. Developed and refined over more than two decades—with roots in Linux Virtual Server technology dating to 1997—SDVN has been deployed in carrier-grade telecom, banking, and enterprise environments serving millions of users.

4.1 Architectural Overview

SDVN achieves its capabilities through a clean separation of the control plane and data plane, enabling centralized policy orchestration with distributed forwarding.

Control Plane

The control plane manages identity lifecycle, authentication, authorization, routing decisions, and network slicing policies. It serves as the intelligence layer that determines how data should flow based on identity, policy, and real-time network conditions.

Data Plane

The data plane performs encrypted packet encapsulation, intelligent next-hop routing, and edge-based forwarding. It operates at the kernel level, integrating components including ACL and connection tracking, virtual routing (vRoute), virtual DNS (vDNS), flow tables, protocol stacks, traffic shaping, and a packet processor with dedicated crypto and compression devices.

Global Overlay Layer

A virtual addressing system provides virtual IP (vIP) and virtual DNS (vDNS) addressing that operates independently of ISP routing. This means every SDVN node has a stable, globally routable identity regardless of its physical location, NAT configuration, or ISP.

4.2 Core Technical Capabilities

Encrypted Overlay Transport

All data transmitted through SDVN undergoes multi-layer packet encryption with dynamic session key negotiation. The system supports AES-256, ChaCha20, and proprietary encryption algorithms. At the source node, data from the application layer is encrypted, repackaged with virtual IP addressing, and transmitted over UDP. At the destination, it is decrypted and handed seamlessly to the application layer. Applications see normal sockets while SDVN handles all security and routing transparently.

Identity-Centric Networking

SDVN implements a dual-layer identity architecture that is central to its security model:

- **Public Identity:** Used for intelligent addressing and routing within the SDVN network. This serves as the user's unique roaming identity across the entire network and can be customized. Public identity includes Owner ID, virtual domain name, avatar, and wallet/billing information.
- **Private Identity:** Contains permissions, service attributes, data ownership, and service properties. Private identity data remains segregated across different virtual subnets and service nodes, never exposed to any third party—including SDVN routing infrastructure itself.

Each packet carries embedded identity and permission data, preventing theft, hijacking, or unauthorized interception. Users access target nodes simply by using the target's virtual DNS name; the SDVN kernel handles all path selection and addressing automatically.

Intelligent Network Slicing

Network slicing enables policy-driven logical segmentation of the SDVN fabric into independent virtual networks, each with dedicated policies, QoS parameters, and security boundaries. Each slice operates as a fully isolated private network with its own access control, billing, and performance profiles. This capability delivers four key benefits:

- **Data Control:** Dedicated networks fully separated from the rest of the SDVN network for data and security containment.
- **Security:** Per-network control over access policies, QoS, and billing—only authorized users and devices can connect.
- **Performance:** Per-network optimization of bandwidth, latency, and reliability.
- **Cost Efficiency:** Shared infrastructure with per-network policies maximizes utilization, while software-defined changes are fast and low-cost.

Distributed Multi-Path Routing

SDVN provides two primary data transport paths: Direct Link Transport (DLT) for globally distributed P2P, P2N, and N2N direct communication, and Forward routing through core and edge nodes when direct paths are unavailable. The system intelligently orchestrates optimal communication paths, provides automatic failover, supports bandwidth aggregation across multiple links, and enables edge forwarding for accessing local network and Internet resources through remote devices.

5. How SDVN Powers the DASSET Storage Platform

SDVN is not an auxiliary feature layered onto the DASSET platform—it is the foundational networking substrate that makes sovereign, user-owned data infrastructure possible. Within the DASSET architecture, SDVN operates as the Network Layer, sitting beneath the Model Service Layer and Application Layer, providing four integrated services: SDVN Global Network, E2E Encrypted Tunnels, Identity and Access Management (IAM), and Audit and Policy enforcement.

5.1 Every Storage Node Becomes a Secure Network Node

Traditional storage systems depend on external networking infrastructure—VPNs, cloud relay services, DDNS providers, or port forwarding configurations—to enable remote access. These external dependencies create complexity, fragility, and security vulnerabilities.

With SDVN integration, every DASSET device is simultaneously a storage node and a secure, identity-bound network node. The storage device itself participates in the SDVN overlay network, maintaining its own virtual IP address, virtual DNS name, and cryptographic identity. This means:

- **Zero Configuration Remote Access:** Users access their DASSET device from anywhere in the world by simply using its virtual DNS name. No VPN setup, no port forwarding, no DDNS subscriptions.
- **No Cloud Dependency:** Remote access does not route through any centralized relay server. Connections are established directly between endpoints through the SDVN overlay, or through edge forwarding nodes when direct paths are not available.
- **Persistent Identity:** The device's virtual identity remains stable regardless of changes to its physical IP address, ISP, or network environment. Users moving their DASSET device to a new location need not reconfigure anything.

5.2 Encrypted Peer-to-Peer Data Replication

Data replication between DASSET nodes is one of the platform's most critical functions—enabling backup, redundancy, and distributed storage across multiple physical locations. SDVN makes this replication inherently secure.

When two DASSET devices replicate data, the transfer occurs through SDVN encrypted tunnels using AES-256 or ChaCha20 encryption. The data is encapsulated with virtual IP addressing and transmitted over encrypted UDP channels. Neither the ISP, any intermediate network infrastructure, nor any SDVN routing nodes can inspect the content of the replication traffic. This provides true end-to-end encryption for data in transit between storage nodes without requiring separate VPN tunnels or TLS configurations.

5.3 Network Slicing for Data Governance

SDVN's network slicing capability maps directly to DASSET's data governance requirements:

- **Family Networks:** A household can create an isolated SDVN slice encompassing all family DASSET devices. Photos, documents, and backups replicate only within this slice. No external device can access the family network without explicit authorization.
- **Business Compliance:** An organization can define network slices with geo-fencing policies that ensure data replication occurs only between nodes in compliant jurisdictions. This supports GDPR, data residency requirements, and industry-specific regulations.
- **Multi-Tenant Isolation:** In managed deployment scenarios, each tenant's data traffic is fully isolated from other tenants—enforced at the network layer, not just the application layer. This provides a fundamentally stronger isolation guarantee.
- **AI Workflow Segregation:** Sensitive AI workloads can be confined to specific network slices, ensuring that model training data, inference requests, and results never traverse unauthorized network paths.

5.4 AI-Aware Traffic Prioritization

DASSET Pro supports on-device AI inference with discrete GPU and advanced AI model support. SDVN's programmable network fabric enables intelligent traffic prioritization that is aware of AI workloads. When a DASSET Pro device is running local inference, SDVN can prioritize AI-related data flows—such as model updates, RAG (Retrieval-Augmented Generation) data retrieval, or distributed inference coordination—over routine storage synchronization traffic. This ensures that AI workloads receive the network performance they require without manual QoS configuration.

5.5 Sovereign Mesh Clustering

Multiple DASSET devices connected through SDVN naturally form a sovereign mesh cluster—a distributed storage and compute fabric that operates under the owner's exclusive control. Unlike cloud-managed clusters that depend on provider infrastructure, DASSET mesh clusters are self-governing. The SDVN overlay provides the encrypted, identity-verified communication channels that bind the cluster together, while network slicing ensures the cluster's traffic is isolated from all other network activity. This architecture enables organizations to deploy distributed, load-balanced, on-premises infrastructure with cloud-like convenience and enterprise-grade resilience.

6. Security Architecture

The integration of SDVN into the DASSET platform creates a comprehensive security model that protects data at rest, in transit, and in topology. This section details the security architecture across six dimensions: access control, encryption, trust evaluation, audit, threat defense, and privacy guarantees.

6.1 Zero-Trust Access Model

SDVN implements a zero-trust architecture where no device or user is trusted by default, regardless of network location. Every access request is authenticated via the SDVN identity system, authorized against slice-level policy, encrypted before transmission, and continuously evaluated throughout the session lifecycle.

Service ports are never exposed to the public Internet. SDVN uses SPA-style (Single Packet Authorization) techniques to ensure that unauthorized parties cannot even discover that a DASSET device exists on the network.

6.2 Multi-Layer Encryption

Data protection operates at multiple levels simultaneously, ensuring that compromising any single layer does not expose the system:

Layer	Protection Mechanism
Storage	AES-256 encryption at rest
Transport	AES-256 / ChaCha20 encrypted UDP tunnels
Packet	Identity-bound encapsulation per packet
Session	Ephemeral key negotiation (forward secrecy)
Topology	Virtual IP / Virtual DNS abstraction
Slice	Logical network isolation at routing layer

6.3 Continuous Trust Evaluation

Unlike traditional access control that grants access once and assumes continued trust, SDVN performs continuous trust evaluation throughout the lifecycle of every connection. The system validates identity integrity, behavioral consistency, policy compliance, and network state on an ongoing basis. Anomalous behavior can trigger re-authentication, permission reduction, or immediate session termination. This prevents lateral movement and long-duration exploitation—two of the most common vectors in modern network attacks.

6.4 Full Lifecycle Audit Logging

SDVN provides comprehensive audit and monitoring at all network layers. Every connection attempt, authentication event, policy decision, and data transfer session is logged with full identity context. This supports regulatory compliance (GDPR, HIPAA, financial regulations), enterprise audit requirements, forensic investigation, and real-time operational visibility.

6.5 Explicit Threat Model and Security Guarantees

SDVN-powered DASSET is designed to defend against defined classes of threats across four categories.

Network-Level Threats

Threats including ISP traffic inspection, metadata surveillance, man-in-the-middle attacks, DNS spoofing, IP hijacking, NAT traversal exploitation, and port scanning are mitigated through end-to-end AES-256/ChaCha20 encryption, virtual DNS (vDNS) independent of public DNS, the absence of exposed listening ports, SPA-style pre-authentication, packet-level identity validation, and encrypted UDP overlay transport.

Cloud Dependency Threats

Threats including centralized relay interception, cloud account compromise, provider-level data visibility, and government subpoena exposure via hyperscaler are mitigated by SDVN's architecture, which requires no relay servers, establishes direct endpoint-to-endpoint encrypted tunnels, and routes traffic through no provider-controlled path. Critically, PlanetX Labs does not store user content, inspect user payload, control user encryption keys, or possess decryption capability.

Insider and Lateral Movement Threats

Flat LAN exploitation, cross-tenant privilege escalation, and compromised device propagation are addressed through identity-bound packet validation, per-slice isolation, a default-deny posture, continuous trust evaluation, and transport-layer micro-segmentation. Every packet must carry valid identity credentials, and network slices prevent any lateral movement between isolated environments.

AI Privacy Risks

Model training data leakage, prompt injection exposure, and cross-tenant inference contamination are mitigated through local inference by default, slice-constrained AI traffic, identity-scoped model execution, and an optional offline AI mode that operates with no network connectivity whatsoever.

6.6 Privacy as Architecture

Most platforms promise privacy through policy. DASSET enforces privacy through architecture. This distinction is fundamental: policies can be changed by providers, overridden by legal requests, or

weakened through corporate acquisitions. Architectural privacy guarantees are structural—they cannot be bypassed without rebuilding the system itself.

SDVN-powered DASSET delivers the following architectural privacy guarantees:

- Data never leaves user-controlled nodes unless explicitly authorized.
- Replication is identity-scoped and slice-constrained.
- Encryption keys are negotiated per session—no static shared master keys.
- No centralized metadata aggregation of user content.
- Virtual identities do not expose physical IP or geographic location.
- Routing nodes cannot decrypt payload content.
- Private identity data is never exposed to SDVN infrastructure.

The result is privacy from providers, privacy from infrastructure, and privacy from network topology—enforced at every layer of the system.

6.7 Cryptographic Design Principles

The cryptographic architecture underlying SDVN follows high-assurance design principles that elevate it beyond consumer-grade VPN architecture into infrastructure-grade territory:

- Forward secrecy via dynamic session keys—compromising one session reveals nothing about others.
- No static shared master keys that could serve as a single point of compromise.
- Kernel-level encryption implementation for performance and tamper resistance.
- Zero plaintext routing metadata exposure—even routing data is protected.
- No trust assumption of ISP infrastructure at any point in the data path.
- Strict separation of identity and routing layers, preventing correlation attacks.

7. SDVN vs. Traditional Approaches

The following comparison illustrates why SDVN represents a fundamentally different approach to storage networking compared to conventional solutions.

Capability	DASSET + SDVN	Cloud + VPN / P2P
Remote Access	Virtual IP/DNS addressing; stable, zero-config, global	Requires VPN, DDNS, port forwarding, or cloud relay
Private Networking	On-demand programmable network slices with full isolation	Flat peer network or provider-managed VPC
Encryption	Kernel-level E2E encryption (AES-256, ChaCha20) on all traffic	Application-layer TLS; VPN tunnels add latency
Identity Model	Dual-layer (public/private) identity embedded in every packet	Username/password or certificate-based; no packet-level identity
Performance	DLT direct paths; intelligent multi-path routing to physical bandwidth limit	Limited by cloud relay or P2P NAT traversal
Data Sovereignty	Geo-fenced routing, per-slice compliance policies	Provider-dependent; limited geographic control
Scalability	Carrier-grade, millions of nodes, decade of production deployment	Cloud-dependent scaling; P2P limited by discovery
Cost	Low infrastructure cost; bandwidth + minimal server resources	High cloud costs; multiple data centers required

7.1 Structural Data Sovereignty

Beyond the point-by-point comparison, SDVN enables structural data sovereignty through capabilities that have no equivalent in traditional approaches: policy-defined replication boundaries, geo-fencing at the routing layer, slice-constrained cross-border enforcement, jurisdiction-aware data routing, and compliance-ready audit logging for GDPR, HIPAA, and financial regulations. Unlike hyperscaler VPC architectures, these controls operate at the transport layer—not just the application layer.

7.2 Four-Layer Defensibility

SDVN-powered DASSET delivers defensibility across four integrated layers that most competitors address in isolation:

- **Network Layer:** Proprietary overlay routing and identity embedding.
- **Storage Layer:** OS-level integrated storage fabric.
- **AI Layer:** Local inference with network-aware optimization.

- **Architecture Layer:** Privacy-by-design structural guarantees.

Most competitors operate at only one of these layers. DASSET's integration across all four creates a compounding advantage that is difficult to replicate piecemeal.

8. Deployment and Partner Integration

SDVN's integration into the DASSET platform is designed for flexible deployment across diverse partner and use-case scenarios. PlanetX Labs provides three deployment models.

8.1 Client SDK

Cross-platform SDKs for Windows, macOS, iOS, Android, and Linux enable any client application to interact with the SDVN network. The SDK provides interfaces for login/logoff, connectivity status monitoring, account and device information retrieval, virtual network enumeration, and forwarding node specification. This allows OEM partners to embed SDVN connectivity directly into their own applications.

8.2 Hosting Model

For SDVN-enabled products that do not require their own management platform, PlanetX Labs provides centralized management through its SDVN cloud platform. This includes account and device management, device-account binding, billing policy enforcement, and operational monitoring. Partners benefit from turnkey deployment without the need to build and operate network management infrastructure.

8.3 Federation Model

For partners requiring independent operational control, PlanetX Labs provides SDKs, technical support, and customized solutions to build and operate their own SDVN management platforms. This model is designed for large enterprises and OEM partners who need to integrate SDVN into their existing infrastructure and management frameworks while maintaining full operational sovereignty.

8.4 Proven at Enterprise Scale

SDVN's architecture has been validated through production deployments across multiple sectors. In carrier environments, SDVN gateway clusters deployed in data centers provide unified identity, encrypted traffic, and centralized authentication across branches and remote workers—eliminating unencrypted inter-branch traffic and weak access controls. In large enterprise deployments, SDVN has secured core applications for organizations with over 200,000 users on unmanaged mobile devices, enabling multi-cloud interconnection, global virtual network access, and high-speed cross-operator connectivity. In personal cloud deployments, SDVN SDK integration enables seamless remote access between personal devices with encrypted tunnels, with account and device binding securely synchronized between OEM cloud platforms and the SDVN cloud.

9. The DASSET Product Portfolio

Every DASSET device is a private data vault. AI capabilities are optional; data ownership is the default. The portfolio is designed to serve the full spectrum from cost-conscious consumers to advanced developers.

Product	Description	Target Audience
DASSET Simple	Entry-level LAN storage with upgrade path to SDVN connectivity	Cost-conscious consumers and SMBs
DASSET Standard	Internet-connected storage with local AI capabilities and app marketplace	Consumers and small-to-medium businesses
DASSET Pro	High-end platform with discrete GPU, advanced AI models, up to 240TB storage, 192GB memory, Intel Ultra 9 processor	Developers, tech enthusiasts, and enterprises
DASSET Desktop	Software that transforms any existing PC into intelligent SDVN-connected storage	Consumers and SMBs seeking to repurpose existing hardware

10. Strategic Positioning

It is important to understand what SDVN is not. SDVN is not a VPN—it does not merely encrypt a tunnel between two endpoints. It is not SD-WAN—it does not optimize traffic across existing WAN links. It is not a blockchain—it does not rely on distributed consensus for trust.

SDVN is a programmable, identity-native, encrypted global overlay network. When integrated with storage infrastructure like DASSET, it becomes the networking substrate for user-owned data and sovereign AI infrastructure. This combination creates a new category: the sovereign edge data platform.

The implications are significant. Cloud solved the scale problem but introduced centralization and data exposure as systemic trade-offs. SDVN-powered storage restores sovereignty, determinism, and identity control to modern digital infrastructure. As data ownership becomes foundational to the AI economy—as the value of data increasingly derives from the intelligence that can be extracted from it locally—the platform that secures data while enabling private AI processing at the edge will define the next generation of data infrastructure.

11. Conclusion

The integration of SDVN into the DASSET platform represents more than a technical enhancement—it is an architectural decision that redefines what storage infrastructure can be. By embedding identity, encryption, routing intelligence, and network segmentation directly into the storage fabric, PlanetX Labs has created a platform where data sovereignty is not an aspiration but a structural guarantee.

Every DASSET device, from the entry-level Simple to the AI-powered Pro, inherits the security, accessibility, and governance capabilities of the SDVN network. Data is protected at rest by on-device encryption, in transit by SDVN tunnel encryption, in topology by identity-verified network slicing, and in identity by dual-layer authentication embedded in every packet.

Cloud solved scale but introduced systemic centralization. SDVN-powered DASSET restores sovereignty, determinism, identity control, and architectural privacy. As the AI economy evolves toward distributed edge intelligence, the infrastructure that secures and governs data locally will define the next generation of digital systems.

For partners, enterprises, and individuals seeking to take control of their data destiny—to build infrastructure where intelligence lives at the edge, privacy is the default, and data works for its owner—DASSET powered by SDVN provides the foundation.

Your DATA | Your ASSET | Your AI

Contact

Partnership Discussions

Jane Cui, CEO

jane@planetxlabs.com

Technical Integration

Kevin Wu

kevin@planetxlabs.com

www.planetxlabs.io