

## DATA SHEET

# Kinnami AmiShare™

## Resilient Data Everywhere

Future-proofed edge computing  
Cybersecurity

[Protects the data not just devices  
& servers]

Availability in Any Environment

[From Edge device to the Cloud  
Network & storage agnostic]

Protection & Security

[Distributed, encrypted, fragmented  
storage. Protect from data loss,  
tampering or theft anywhere]

Immutable Data Authenticity

[Auditable, traceable, versioned,  
lasting]

Autonomous, Unstable

Environments & Networks  
[Replication and versioning provide  
redundancy for autonomous operation  
& data recovery]

Intelligent Policy Engine

[Adapts & optimizes based on usage  
patterns in real-time]

## Hybrid Resilient Data Fabric: Kinnami AmiShare™ transforms data protection for our digital world.

Data must be managed in this complex, hybrid world where data resides in your data center, in the cloud, at the edge, and through externally linked applications and platforms. The growth and manageability of data needs to be effectively governed to ensure data sovereignty, integrity, security, and privacy are maintained.

Kinnami Hybrid Resilient Data Fabric is a unified way to manage data availability, protection, security, and ownership. AmiShare automates an otherwise complex process and eliminates the patchwork of systems required to deliver resilient data today.

### 01 Data Owners & Administrators

Kinnami takes a Zero Trust approach toward protection and securing your data. We separate data ownership and privacy from the administration of policy. The administrator's role is to administer policy as defined by your organization. Administrative policy manages where and when data are stored, who may access it, and who may collaborate with whom. Administrators are unable to access the data themselves.

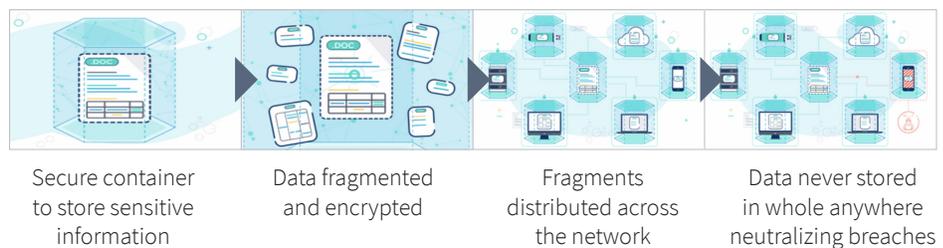
AmiShare separates the capabilities of data owners, who create, modify and otherwise use data, from system administrators, who define and administer policy. Data privacy is kept at the ownership-level—secure from tampering, even by those with administrative rights. This way highly sensitive information is always protected no matter where it resides.

This separation of operational responsibilities more closely matches the different business priorities of data owners and administrators providing better security overall.

### 02 Protection and Security

Data is secured at its origin. Immediately after new data is created, it is split into fragments. The fragments are encrypted uniquely and stored where they were created. The data is then replicated and distributed according to defined policy. Then these encrypted fragments are transmitted across the network to storage devices defined by the administrators' policies.

#### Fragmented, Encrypted, Distributed



Trustworthy, reliable data is available on any network, using any type of storage—even in real-time and in unstable network environments. Ownership is preserved and protected even in networks you may not control.

# Resilient — Protection, Access Control, Threat Detection & Investigation

## Any network, any storage

### 03 Audit System

Using metadata about the users, the stores and the data, policies define goals for the distributed storage system to decide which stores hold what fragments. When the policy or environment change, fragments are moved around the network to reflect the new state. This creates a resilient, immutable, auditable data fabric.

AmiShare's access subsystem surveils and audits the entire computer for data leaks or other unusual behavior. Threat detection systems can use this information to detect anomalies such as a user off-loading large datasets, which can drive access policy rules. All this increases system administrator's visibility into users' behavior, without needing access to the end-user's data.

AmiShare's auditing system tracks end-user operations at access points and storage locations as well as administrative operations assuring data remains confidential. Versioning provides a complete audit trail. AmiShare provides proof of data authenticity.

Audit information can be transferred to external threat detection systems to improve their accuracy and capability. AmiShare's policy engine can work with external threat detection systems to determine where fragments are stored and to automate the security response to attacks.

### 04 Smart Data Movement

AmiShare automatically controls access and movement of data. Data is moved to the most reliable and efficient storage based on demand and conditions such as bandwidth. Data is always available and automatically optimized for cost. In cases where bandwidth is not reliable, data can be moved in advance of its use and available for use when needed.

Kinnami AmiShare automatically moves data and controls access to stay compliant. Data access can even be aligned with parameters such as GPS to keep GDPR compliant, or calendar apps which can identify scheduled travel and proactively move data.

### 05 Intelligent Policy Engine

The policy engine automates intelligent distribution of data and optimizes for data resilience. System administrators only need to align policy for storage devices according to attributes such as physical security, location and ownership, the policy engine does the rest.

Policy definitions are dynamic. Our security & auditing tools are specifically built to assess data security including tracking data owners and administrator behavior. Data access patterns are identified and used to develop and implement threat detection policies. This way user access can be cut-off immediately in the event of an anomaly. Administering policy for third-party tools is also easier.

#### Environments

- Distributed networks & storage
- Peer-to-peer networks
- IoT Edge devices
- Autonomous
- Unsecured networks

#### Secure & Protected

- Smart data movement
- Client-side encryption
- Replication & versioning
- Auto-data recovery
- GDPR/Compliance