KINNAMI

Software Corporation

WHITEPAPER: KINNAMI TECHNOLOGY OVERVIEW

Introduction

Traditionally, data collected at the edge has been sent back to data centers, where it is processed, and then the results are pushed back to the edge if and when it is needed. This old paradigm does not quite work anymore. The world we are now building is distributed, and increasingly reliant on (if not requiring) data processing at the computing edge on drones, satellites, autonomous vehicles, IoT/sensors and other connected devices and applications.

Gartner estimates that by 2025, 75% of all data will be generated and processed at the computing edge, up from just under 10% in 2018. This massive shift in where and how data will be used requires a very different data management and security infrastructure to what is available today. While companies like Amazon Web Services (AWS), Microsoft, and Google enable secure data storage and management in the Cloud and companies like Symantec and Forcepoint provide endpoint security solutions, there is no one providing the same across a distributed network, from sensors at the edge, to workstations, to servers in datacenters and to the cloud. This requires a resilient hybrid data fabric. That is what we uniquely do at Kinnami.

Whether in smart manufacturing, autonomous systems, space applications, or even defense operations, enterprises today need better solutions that can securely automate data distribution to the computing edge (on satellites, aircraft, drones, autonomous systems, personnel devices, IoT/sensors, and other endpoint devices like laptops, mobiles, and even removable drives) especially when network communications are degraded. These data must be securely moved to and securely stored wherever they are needed, on whatever device is available, across different levels of security.

Kinnami Technology Overview

Kinnami's technology is aimed at organizations that need to protect sensitive information on storage devices and access points that are often beyond an organization's control (i.e. under centralized IT control), driven by modern needs for data processing and data sharing that extend across company boundaries and at the computing edge.

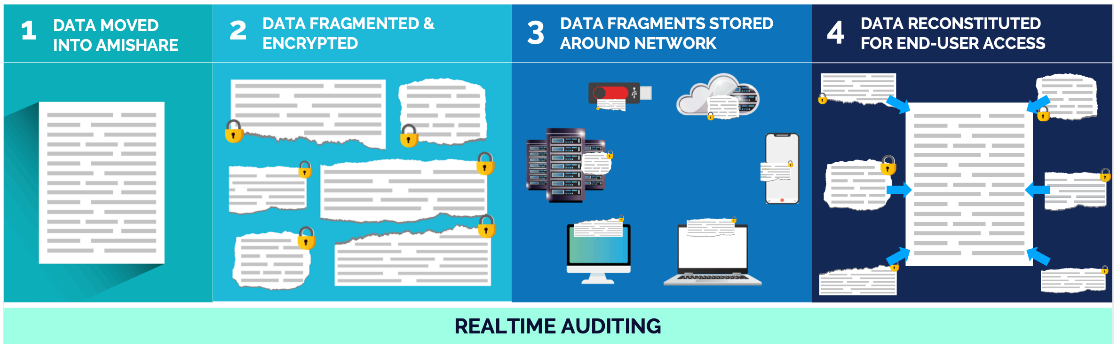
Kinnami is a resilient distributed data management company that provides organizations what they need to secure and protect sensitive information at the computing edge.

Starting with a distributed storage subsystem, our Kinnami AmiShare™ platform safeguards sensitive information regardless of where it is accessed or who is accessing it. Our mission is to deliver innovative solutions to facilitate efficient collaboration using secure information storage and access on multiple devices especially at the computing edge - endpoints with their inherently weaker security and mobility - as well in datacenters. These include cloud services, laptops, mobile phones, IoT devices & removable disks.

AmiShare separates the capabilities of end-users, who create, modify and otherwise use data, from system administrators, who define policies that specify where and when data are stored, who may access it, and who may collaborate with whom. But most importantly, administrators are unable to access the data themselves. This separation of operational responsibilities more closely matches the different business priorities of end-users and administrators, leading to less "Shadow IT" and better security overall.

Immediately after a new datum has been created, it is split into fragments. The fragments are encrypted uniquely and stored where they were created. Subsequently, these encrypted fragments are transmitted across the network to storage devices defined by the administrators' policies. Using metadata about the users, the stores and the data, these policies define goals for the distributed storage system to decide which stores store which fragments. For example, a policy may forbid a datum's fragments from being partially or entirely stored on a particular laptop, protecting the datum's security. If the policy or environment change, which can happen at any time, fragments are moved around the network to reflect the new state. Continuing the example, if that laptop is connected to a different network, the fragments may be automatically moved onto the laptop for faster access.

AmiShare's auditing system tracks end-user operations at access points and storage locations as well as administrative operations such as granting and revoking end-user access, assuring the administrators that data are remaining confidential. Audit information can be transferred to external threat detection systems to improve their accuracy and capability while AmiShare's policy engines can work with external threat detection systems to determine where fragments are stored and to automate the security response to attacks.


1 DATA MOVED INTO AMISHARE
2 DATA FRAGMENTED & ENCRYPTED
3 DATA FRAGMENTS STORED AROUND NETWORK
4 DATA RECONSTITUTED FOR END-USER ACCESS
REALTIME AUDITING

Today, there is a patchwork of storage and security solutions that organizations use to manage data security but protecting confidential information has largely been relegated to "all or nothing" device and/or network security. This has resulted in an explosion of the number of data breaches and the associated loss of sensitive data costing organizations millions of dollars in financial losses.

Kinnami Technology Benefits

By integrating user access management, distributed storage management, as well as encryption and auditing, AmiShare offers the following benefits:

1. **Future-proofed edge computing cybersecurity that protects data rather than just devices & servers:** Unlike traditional cybersecurity that focuses solely on protecting devices and servers, AmiShare avoids the "software gate" under privileged control and encrypts data immediately (client-side encryption) before being stored. This protects the information itself regardless of where it is stored or accessed. AmiShare's dynamically configurable platform operates independently on endpoints (laptops/desktops, mobiles), servers (cloud, on-premises), IoT devices, and removable devices (USB sticks, big disk arrays for moving Petabytes and Exabytes of data, or across air-gapped networks). This is essential to protect data at the edge, on unsecured networks, as well as in disconnected/autonomous environments. This is also essential to protect data in hosted environments, such as cloud storage. A recent data breach was hosted on AWS and stolen by an AWS administrative employee.

2. **Distributed encrypted fragmented storage reduces breach risk and improves efficiency:** Enterprises are realizing that "encrypting data at rest or when transmitted" is insufficient, rather data must only be decrypted when & where they are actually being used – a fundamental design principle of AmiShare. AmiShare stores data as fragments that are all individually encrypted with each fragment having its own unique, private encryption key. Administrative policies dictate how these fragments are distributed over a network of devices (servers and/or endpoints). Overall security is improved because the encrypted fragments are not concentrated on one storage device, reducing the value of attacking a particular storage device. Efficiency is improved by minimizing unnecessary data movement across networks, which is very desirable on degraded or over-loaded networks.

3. **Replication and versioning provide redundancy for autonomous operation and data recovery:** Administrative policies define how AmiShare stores multiple copies of fragments on multiple

storage devices to ensure availability even when particular storage devices or the network are unavailable. If desired, all encrypted fragments of a particular datum can be stored on one storage device, allowing autonomous operation. New immutable versions are created as data change, allowing immediate access to older versions, (e.g. after a ransomware attack,) reducing downtime and costs. During DDoS attacks, alternative copies of a fragment can satisfy access requests, mitigating the attack.

4. **Storage agnostic platform:** AmiShare has been designed to take advantage of whatever storage systems customers are using – whether in a datacenter, a cloud solution, an on-premises storage solution, or endpoint devices. It is also easier for customers to be able to switch between storage solutions, unlike current options which make it expensive & time-consuming.

5. **Detailed, focused information for access control, and threat detection & investigation:** AmiShare's design fundamentally assumes that all devices are hostile – its security & auditing tools are specifically built to assess data security in this environment, tracking end-user & administrator behavior. System administrators define policies on a storage device according to attributes such as its physical security, location, ownership, etc. These policy definitions are dynamic, so changes are reflected by changes in the platform's behavior as soon as possible. This information can be used to identify data access patterns and develop threat detection policies (e.g. cut-off user access in event of an anomaly) as well as provides data for 3rd party tools.

6. **Surveillance of endpoints used by end-users for access:** AmiShare's access subsystem surveils and audits the whole computer, not just the data protected by AmiShare, to watch for data leaks and other unusual behavior. Threat detection systems can use this information to detect anomalies (e.g. an end-user off-loading large datasets) which can drive access policy rules. All this increases system administrator's visibility into end-user behavior, despite not having access to the end-user's data.

-END-