About Kinnami Software Corporation

Kinnami Software Corporation provides a resilient distributed data management platform that simplifies data availability, protection, and security for the complex distributed networks that are essential for making the connected future possible and an autonomous future a reality. Kinnami's software enables a unified data environment for trust, transparency, and newfound collaboration from the digital edge to cloud. Customers achieve the irrefutable data integrity essential to distributed environments—including unsecured or free-standing networks and autonomous operations. 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 driven by modern needs for data processing and data sharing that extend across company boundaries and at the computing edge. Kinnami was founded in 2015 by a team of data protection and security experts and has offices in Boston, Washington, Austin, TX, and London.

Introduction

Traditionally, data collected at the digital edge has been sent back to data centers where it is processed and then the results are pushed back to the digital 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 digital edge on drones, satellites, autonomous vehicles, IoT/sensors and other connected devices and applications.

Gartner estimates that by 2025, 50% of all data will be generated and processed at the digital edge, up from just under 10% in 2018. This massive shift in where and how data is used requires a very different data management and security infrastructure from 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 data centers and the cloud. This requires a resilient hybrid data mesh. That is what we do uniquely 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 at the digital edge (on satellites, aircraft, drones, autonomous systems, personnel devices, IoT/sensors, and other endpoint devices such as laptops, mobiles, and even removable drives), especially when network communications are degraded. Data must be securely moved to and securely stored wherever they are needed, on whatever device is available, across different levels of security.

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, that is beyond centralized IT control. This is driven by modern needs for data processing and data sharing that extend across company boundaries and beyond, including the digital edge.

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

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

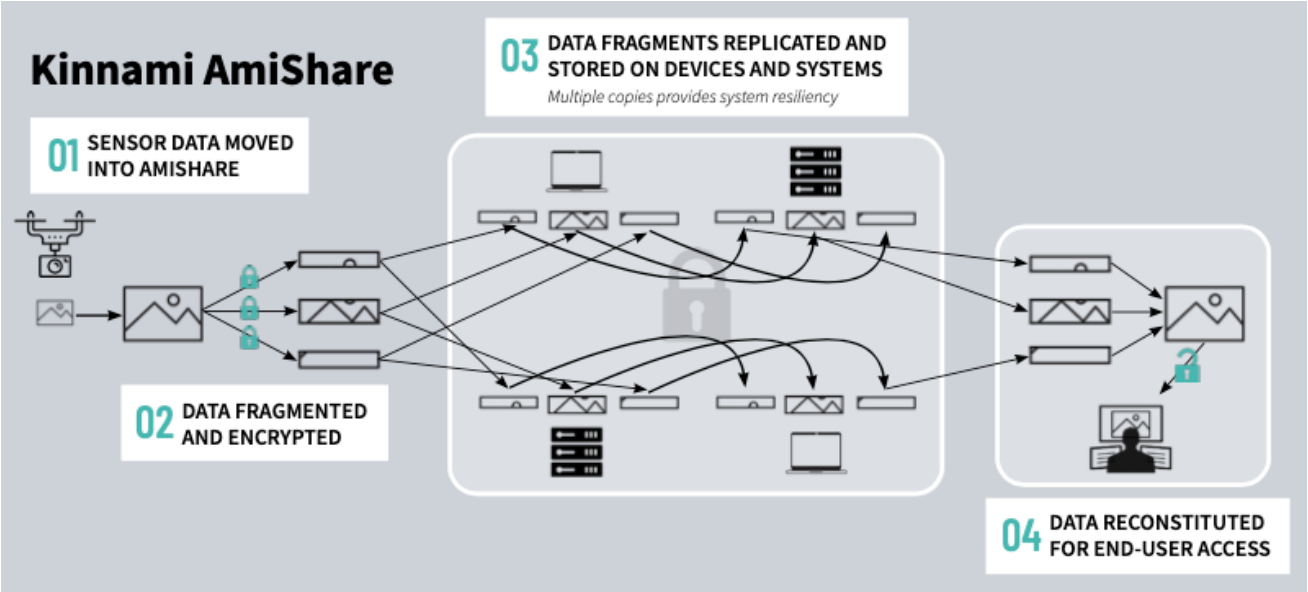
AmiShare separates the capabilities of end-users, who create, modify and otherwise use data, from system administrators, who define policies which specify where and when data are stored, who may access it, and who may collaborate with whom. But most importantly, administrators are unable to access the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

Immediately after a new datum is created, it is split into fragments. The fragments are encrypted uniquely and stored where they are 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 what 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 administrators that data remain confidential. Audit information can be transferred to external threat detection systems to improve their accuracy and capability. 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.



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 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 digital edge, on unsecured networks, and in disconnected or autonomous environments. This is also essential to protect data in hosted environments, such as cloud storage.
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 and where they are actually being used— this is a fundamental design principle of AmiShare. AmiShare stores data as fragments, and each fragment is individually encrypted and has 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 and this reduces 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. Additionally, it is easier for customers to be able to switch between storage solutions, unlike current options which make it expensive and time-consuming.

5. Detailed, focused information for access control, and threat detection and investigation: AmiShare's design fundamentally assumes that all devices are hostile—its security and auditing tools are built specifically to assess data security in this environment, and tracks end-user and 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 a user's access in event of an anomaly) as well as provides data for third-party tools.

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

Conclusion

Innovators need better solutions to securely automate data distribution to the computing edge, especially when network communications are degraded. Data must be securely moved to and securely stored wherever they are needed, on whatever device is available, across different levels of security. The patchwork of storage and security solutions, which supported centralized processing, simply do not work for these complex data environments. Kinnami's distributed data management and security software platform, AmiShare, was developed to provide a resilient distributed data mesh to safeguard sensitive information regardless of where it is accessed or who is accessing it. With AmiShare, organizations can holistically enable data protection, security, and availability. This could be in a data center, in the cloud, or more importantly at the digital edge where networks may be denied or degraded.

KINNAMI