



Akoura products are designed to increase industry adoption rates for information security through technology innovation and improving the experience of the end-user. Akoura provides enterprise users the strongest possible two or three tier end-user authentication and an industry leading information protection technology. Akoura product suite allows users to protect sensitive information wherever it is stored, and whatever the format.

DataSecure Software Solution

DataSecure is a highly scalable, enterprise information protection solution utilizing a very large key encryption, obfuscation, and strong authentication. DataSecure protects any enterprise information at rest, in transit, or in archival. Akoura's core technology transforms the sensitive information into an innocent looking plausible cover. The plausible cover ensures that the "protection" stays with the sensitive information no matter where the information is sent or resides.

DataSecure's strong authentication ensures only authorized, authenticated access to protected information. The Akoura DataSecure solution enables an enterprise to encrypt outbound electronic mail attachments and begin the process of putting in place a robust Secure E-mail Boundary (SEB) solution.

Akoura DataSecure is breakthrough information protection software providing customers unprecedented levels of security. Unlike traditional encryption, Akoura's obfuscation technology leaves no visual or digital signature on the protected information. One of the principal benefits of DataSecure is that it ensures a highly secure, anonymous, storage, archival, or sharing of sensitive information and intellectual property.

How DataSecure Works

DataSecure protects and manages information in a software-based "cryptographic data store" which

can reside on a laptop, desktop, network drive, the web, or a removable media. Each "cryptographic data store" provides a catalog of protected files. Access to the "cryptographic data store" is only provided via strong authentication. Files secured within the container are unknown to the host-device operating system. Strong authentication opens the "cryptographic data store" and allows for secure access to the protected information.

DataSecure also offers a "collaboration" feature – where sensitive information can be secured, obfuscated, and transmitted over any enterprise network or the public internet under plausible cover. Only the intended recipient will be able to decode the information and gain access to the sensitive information with one or two clicks of the mouse.

Once obfuscated, the highly secure plausible cover appears to be no different than an ordinary file. DataSecure leaves no discernable means of determining that sensitive information is contained within the plausible cover.

Unrivaled Benefits

Highly Secure

An innovative combination of encryption, plausible cover technology, and strong authentication provide the highest level of security for information protection. Protected files leave no visual or digital signature and are thus almost impossible to detect. The use of strong authentication eliminates password vulnerabilities.

Reliable

DataSecure is a field tested and commercially available information security software. Akoura has partnered with industry leading vendors to integrate strong authentication with DataSecure.

Unprecedented Security

DataSecure protects sensitive and confidential information regardless of the file type or the host device. Once a file is protected, it can only be retrieved based on strong authentication.



Easy to Use and Install

DataSecure is a simple host-device software application. DataSecure is simple to use and easy to install and deploy. The total time required to install the software application and complete the fingerprint enrollment process is less than fifteen [15] minutes. Akoura's implementation of "drag and drop" encryption is the simplest method commercially available for protecting information. Implementing DataSecure requires zero incremental network or security infrastructure.

Sharing of Protected Files

DataSecure enables users to securely and easily share files over the enterprise network or the public Internet. Once a protected file is identified for "sharing", the file is encrypted within a plausible cover with a click of the mouse. The encrypted file is assigned a private key by the sender and can be sent securely over the enterprise network or the public internet using any email application or platform.

Decoder

The recipient of a DataSecure encrypted document will require the DataSecure Decoder and assigned private key. If the recipient doesn't have the Decoder, it can be easily downloaded from www.akoura.com. The download takes about ten seconds on a high speed connection.

Features and Requirements

DataSecure offers the following features:

- Industry Leading very large key based Encryption
- Undetectable Plausible Cover Technology
- Single User or Enterprise Model
- Strong Authentication
- Dynamic Encryption Algorithms
- Symmetric Key Based Encryption
- Plausible Covers Can Be Stored offsite for Backup and Recovery

The minimum requirements needed to use DataSecure are:

- Windows 2000 or XP
- 256 MB RAM
- 1 GB available disk space
- 1 USB Port

Call us at 781-245-3536 to order your software today or go on our website at www.akoura.com to download more information.

About Akoura

Akoura is located in Cleveland, Ohio. Akoura is dedicated to increase industry adoption rates for information security through technology innovation and improving the experience of the end-user and is committed to developing security solutions that offer the strongest levels of commercially available information protection technology, with zero incremental investment in infrastructure, and a simple, functional end-user experience.

All rights reserved. Akoura, PrivateDisk, DataSecure and MailSecure are trademarks of Akoura Biometrics, Inc.