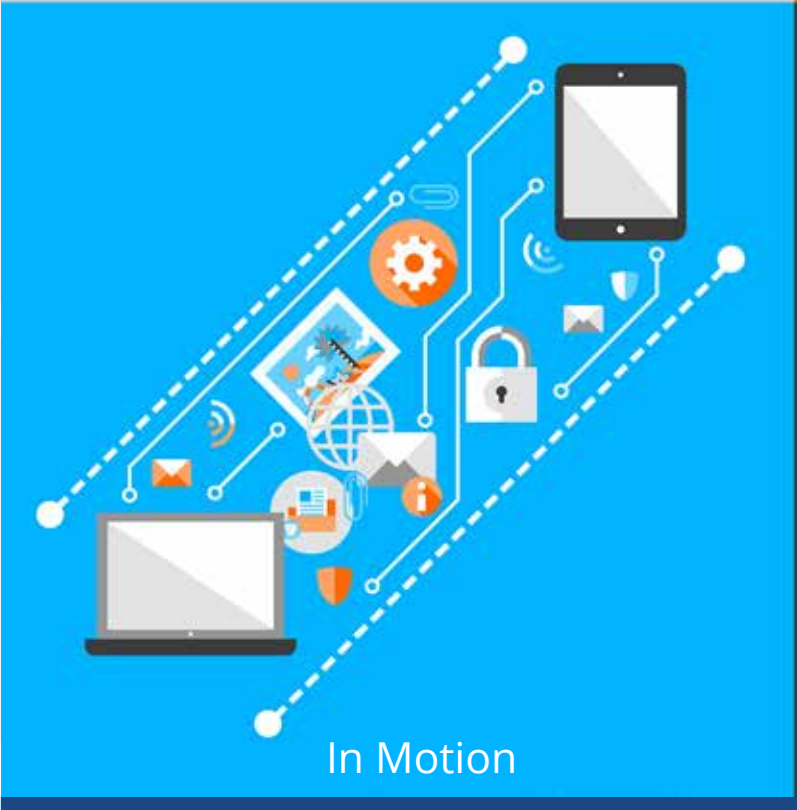
SecureAge

SecureData

Maximum Data Protection

In Use



In Motion

At Rest

Ultimate Defense Built into Every File

What is SecureData?

Automatic File & Folder Encryption

SecureData is a smart, highly flexible, policy-based and end-to-end data encryption solution that protects user data files and folders from data leaks across all types of storage media.

Its unique 3P Technology combined with proprietary Application Whitelisting and Application Binding not only ensures your data remains protected but also remain resistent to the actions of Advanced Persistent Threats (APT), sniffers, and Man-in-the-Middle attacks.

Proactive

Users do not have to consciously remember to encrypt data that the system is processing, ensuring a secure yet natural workflow.

Pervasive

Every file is encrypted no matter where it resides on your system - from creation up to its storage on any location or medium, even the cloud.

Persistent

Every file remains encrypted while travelling over-the-wire, keeping it safe from network sniffers and man-in-the middle attacks.

3P Technology

The basic principle of SecureData is to provide transparent encryption of any data files, which will remain encrypted, whether at rest, in-transit, or in any storage systems. It prevents anyone sniffing the network from obtaining any useful information.

Application Whitelisting

Designed to combat sophisticated Advanced Persistent Threats (APT) and malware attacks, the included Application Whitelisting component smartly creates a complete list of trusted applications that are allowed to run.

This effectively blocks all new executable malware from running and renders existing ones incapable of further infecting a machine.

Application Binding

This ensures that data can be accessed only by specific and authorized applications to keep sensitive data protected from processes potentially compromised by zero-day malware.

Application Binding can also restrict high-risk applications such as browsers from automatically accessing sensitive data without the user's consent, creating an "Application Sandbox" so only files from a specific directory are readable and writeable.

Key Benefits & Technology

Data Privacy without Compromise to Productivity

Require minimum end-user training to ensure data security practices for daily use. SecureData has features that work to enable, not cripple, productivity while defending against insider and outsider attacks.

- Automatic encryption of files at all times including temporary & system page files.
- Complete encryption of data traffic over networks (i.e. network servers & disks).
- One-stop encryption of files created, edited, & copied/moved to any storage device.
- Multiple & simultaneous smart card, USB token, and HSM support.

Straightforward Implementation

Integration of SecureData to various systems applications requires minimal effort and is complemented by the expertise provided by a dedicated support team.

- Easily configurable policy control to support enterprise security needs.
- User specific policy control to provide different security rights for different users.
- Centralized policy updates and log management via web-based console.
- Comprehensive key management support.

Military Grade Security Features

Built to meet the standards of military information security, SecureData incorporates key technologies to deliver unparalleled data protection.

- Default 256-bit AES encryption & Elliptic Curve Cryptography (ECC) for advanced users
- Unlimited key length RSA & DSA
- Multi-user profile management with unlimited user key history support
- Customizable Encryption Algorithm
- PKI optimization with peer certificates local management
- Two-way authenticated TLS/SSL Connection
- Standard X.509 v3 certificate support

Global Regulatory Compliance

Easily achieve regulatory compliance with the world's most discerning legislative requirements on information privacy. SecureData is compliant with the following:

- Payment Card Industry Data Security Standard (PCI DSS)
- Protection of Sensitive Agency Info (White House OMB)
- Sarbanes-Oxley (SOX)
- Health Insurance Portability & Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Monetary Authority of Singapore Technology Risk Management (TRM)
- Various Data Breach Disclosure Bills (i.e. California SB 1386, European E-Privacy Directive)

SecureData Strategic Applications

Anti-APT & Anti-Malware

Featuring an Integrated Application & Data Control (Patented) solution, SecureData's Anti-Malware component detects, wards off and removes known threats such as rootkits, spyware, viruses, trojans and other malicious code while also securing clients against APTs.

The Application Whitelisting component ensures that any stolen data will remain encrypted and useless to attackers. On the other hand, Application Binding mitigates the risk of zero-day attacks by automatically restricting high-risk applications from accessing the user data files without consent from the user.

For Enterprise Servers

Single-handedly safeguard organization's sensitive data that is stored on file servers, enterprise database, Microsoft SharePoint, proprietary enterprise application servers, FTP servers, and backup tapes. Any data stored in the servers are automatically and will remain encrypted as it is moved between servers or client machines.

Enterprise server security can be further enhanced by restricting sensitive data by encrypting them with keys belonging solely to authorized users. This keeps unauthorized users with administrator privileges incapable of a successful insider attack.

For Database Servers

Using file-level encryption, SecureData automatically encrypts both structured data inside the database and unstructured data outside the database. Unlike Column-level encryption and Internal Transparent Data Encryption (TDE), the entire database is encrypted while minimizing operational costs by providing an all-in-one solution.

Since the encryption process is transparent to databases and applications, it does not need to make any changes to the existing database and application while encrypting the data. This greatly increases operational efficiency of database security.

For Cloud Computing

SecureData's unified policy of configuring and imposing protective measures on sensitive data allows incredible flexibility to where data can be stored by ensuring it remains encrypted all the time. This essentially keeps any data stored outside the client's machines, especially those on cloud servers, perfectly secure.

Any attempts by internal and external parties from the cloud operator to steal sensitive data only see encrypted data that cannot be deciphered without the user encryption key.

Need More Information?

www.secureage.com contactus@secureage.com