One-stop
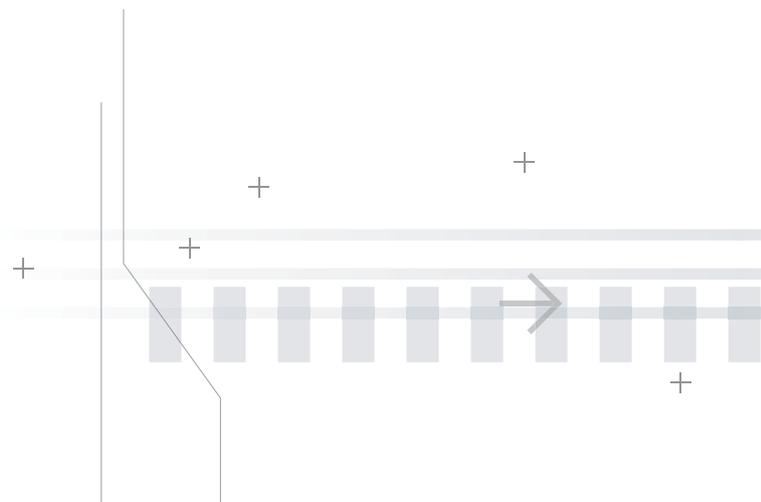## Automatic Data Encryption
Anytime, Anywhere

SecureData
Whitepaper

SecureAge
Data Breach Prevention
Solution

In recent years, major cases of data loss and data leaks are reported almost every week.These include high profile cases like US government losing personal data on 26.5 million veterans on USB disk in May 2006, the discovery in January 2007 of hacking incidents at TJMaxx that compromised 45.7 millions credit and debit card account numbers, and the lost of 25 millions UK citizen personal info and banking details on DVD disks in November 2007. The loss of 130 million credit and debit card account numbers by Heartland Payment Systems in 2009 and the recent massive data breach of user account information by Sony highlight that significant data breach are still occurring to companies, including some that are certified compliance with data security standards. In fact, these reported personal information loss is probably just the tip of the iceberg of sensitive data breaches occurring at organizations throughout the world. Specifically, highly important business information assets like financial information and business trade secrets are frequently lost without them being reported.

How could we prevent such data breaches from occurring? While firewall and antivirus solutions have helped to mitigate against a host of external IT threats, the greatest threat is now very much inside the organization. One major class of security issues is the management of the proliferation of smaller and more powerful mobile and storage devices. Another is the management of the mobile computers that are used outsides the organization but could contain highly sensitive organization information.

There are some solutions on the market that could help organizations manage devices on their network or block gadgets from connecting to their computers. Some solutions require the installation of network servers to block data files from being transmitted from the internal network to external network. Such solutions could help to prevent some accidental data leaks while the enterprise computers are used by non-technical users. A technical user could however easily bypass such security by booting the machine into a different OS via external CD or floppy to copy the hard drive information, or just extract the machine hard drive and access it directly using a USB hard disk enclosure.

Another class of solutions encrypts data on the local hard drive or external storage devices. For instance, the latest Microsoft Vista operation system supports BitLocker Drive Encryption that encrypts the full local hard drive. Such solutions are good for preventing data loss due to the lost of laptop computers or pre-configured encrypted USB drives. The disadvantage to such solutions is that once you enter the password, your computer would no longer be protected from remote and malware attacks, or from physical access if the computer is left unattended. It is also generally not very useful in preventing the attacks of a disgruntled employee or a malicious virus program from copying sensitive information over the network – either to a network connected external drive or sending the data over an email, webpage upload, IM traffic or other network programs. In general, such encryption solutions are point solutions that are limited in the types of storage devices they support, e.g. most solutions only encrypt the local hard drive, or external USB drives but not both. Consequently, they open up "holes" in the system infrastructure to allow easy copying of sensitive information to external storage devices without leaving a trace.

In order to provide a total security against data breach, a single end-to-end data protection solution is needed to safeguard important organization information without having to combine a host of different solutions to stop data leaks from different channels. A single solution also entails a unified policy could be imposed to protect sensitive data from being compromised regardless of where the data is stored; be it on local hard drive, network file server, data tapes, USB drives, CD/DVD, and even yet-to-be-invented future storage devices.

SecureData System is the latest innovation in the SecureAge family of data security solutions. It helps to enforce data privacy requirements as well as preventing data loss and data leaks of sensitive personal information
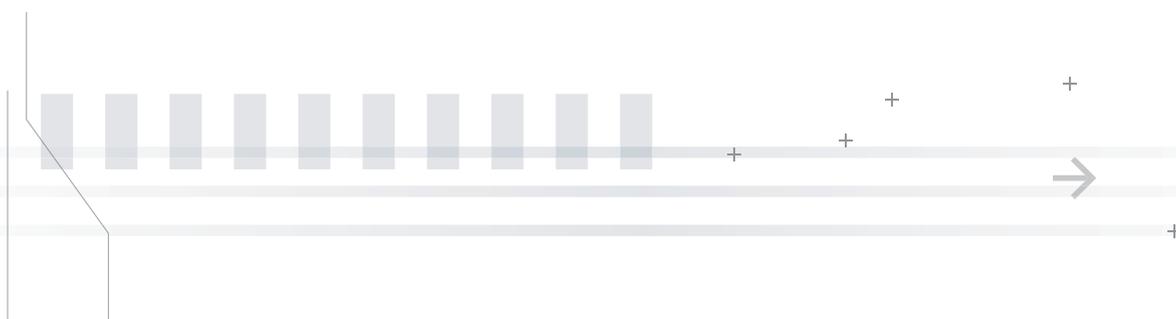
and valuable enterprise information assets.

The basic design principle of SecureData is to provide transparent encryption for any user data files regardless of its storage media. Any data files that are created, edited, moved, or copied to any local, external or network storage devices are automatically encrypted based on pre-defined policy. Without changing the way the users make use of their computers, SecureData transparently ensures all important documents and data files are stored in encrypted format. Consequently, when users lost their laptops or portable storage devices, there is no risk of compromising the sensitive information stored on these devices. Furthermore, even when the machines are up and running, any unauthorized copying of sensitive documents from a desktops, laptops or fileservers will only expose encrypted data files and the risk of sensitive information leaking is thus mitigated.

Network storage devices are one aspect of storage security that is frequently ignored by other data security solutions. With the desire for centralized data management and the ever improving storage capacity of external storage devices, more and more sensitive data in organizations are now distributed over the networks with the user desktop or laptop being regarded as just one of the many network storage devices. However, these distributed data files are usually not protected. Specifically, once a network drive is shared across the network, its data files could be read in clear over the network – even if the shared hard drive is fully encrypted. Consequently, data files on network file server or local files on user machine shared across network could leak out easily.

SecureData resolves this network security issue by ensuring that files written to network file server are automatically encrypted on user machine before they are transmitted over the network. In addition, if the local drive of a machine is shared across the network, the transmission of the user data files will remain encrypted over the network and only authorized recipients with the appropriate keys could decrypt the data files on-the-fly. One benefit of this end-to-end security architecture is that anyone sniffing the network traffic (which could be easily accomplished on a public wireless network) will not obtain

any useful information. One data breach incident highlights the important of end-to-end security – Hannaford Bros. Co, an American supermarket chain lost 4.2 millions credit card data in March 2008. Hannaford has been certified PCI DSS compliant before the attack occurred and their credit card data are encrypted on server. The investigation following the attack found that network sniffer software was installed on their internal network server and it defeats the point encryption solution that Hannaford had put in place.

Additional features of SecureData include device blocking and application binding. Device blocking could be used to impose policy like restricting the usage of certain devices, e.g. allowing reading of data stored on CD/DVD but blocking writing data to them even if then CD/DVD drive and media are writable. Application binding allows highly sensitive documents to be bind to certain applications so that only such applications can access these documents transparently while unauthorized applications or virus programs would be blocked from accessing these documents. For instance, one could create policy to ensure that highly valuable electronics circuit design file could be edited by authorized employee even when working off-line from home but restrict the same employee from leaking the file to other unauthorized external parties.

Like all important data, sensitive data files that are encrypted need to be properly backup so that they could be recovered later. For virtual volume or full disk encryption, the only way to safely backup the files in encrypted format would be to copy the full disk image which would take up enormous storage space. With SecureData, the data backup operation could be performed in the usual fashion with standard backup software. Individual files will remain encrypted in the backup media and fully protected from unauthorized access even if the media is lost. One could also perform daily incremental backups of files that have changed to significantly reduce the backup storage requirement.

SecureData leverages the comprehensive suite of security features of the SecureAge platform to provide state-of-the-art security protection for the users. Specifically, SecureData encryption is based on the
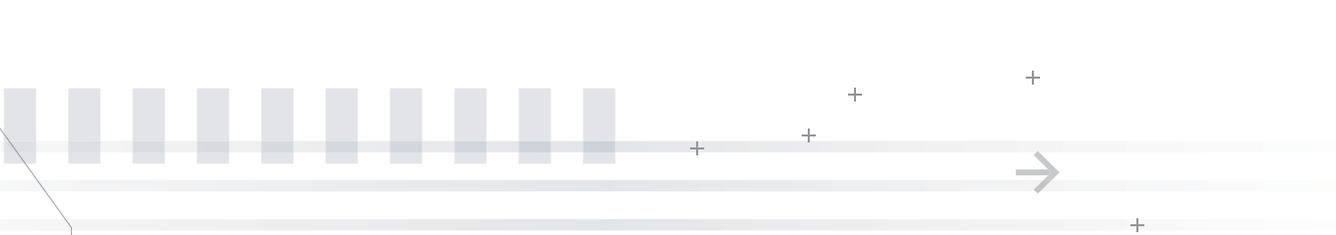
strongest AES algorithm with each data file protected by a different randomly generated 256-bit AES session key. The session key is in turn protected by the user's RSA public key with key strength of 1024, 2048, 4096 or higher bit length. Advanced user could also opt for Elliptic Curve (ECC) public key system or DSA instead of RSA to improve the key efficiency. The user's public and private keys can be stored on any PKCS#11-compliance smart card or USB token to provide strong 2-factor protection. The

usage of public key cryptography also allows sensitive data files to be easily shared by any dynamic group of authorized users without having to put in place a complex key management system.

A policy wizard is available for system administrator to configure the privileges of individual users within an organization in terms of who has the authority to transmit plain document to external parties or decrypt information on external storage media. In combination with the SecureAge central management server, this enables an organization to create user specific policies for all their users for both on-line and off-line usages. The server could centrally control the SecureData policy for each user and

also allows dynamic update of the user privileges on a long term or per-session basis.

In addition to protecting data files by encryption, SecureData provides complete data access audit log. It could be configured to provide different level of details of data access log entries to fit individual enterprise requirements. The audit trail could provide detailed information of every file access by different application, moving of information to external devices, file ownership information, and blocked operations. The SecureAge central management server automatically consolidates all user log entries to provide a consolidated view of user activities and raises alerts when it detects undesirable file access activities.

SecureData provides an end-to-end data breach prevention solution to safeguard sensitive organization information from leaking out. It helps to reduce the cost of data breach prevention by offering a single complete data protection solution for all storage devices. Its total transparent operations ensure the users would enjoy the added layer of security it provides without being inconvenient by it.