

The
Secure Data
Solution[®]

Protected by U.S. Patent 7,293,179;
European Patent 1669872;
and others pending

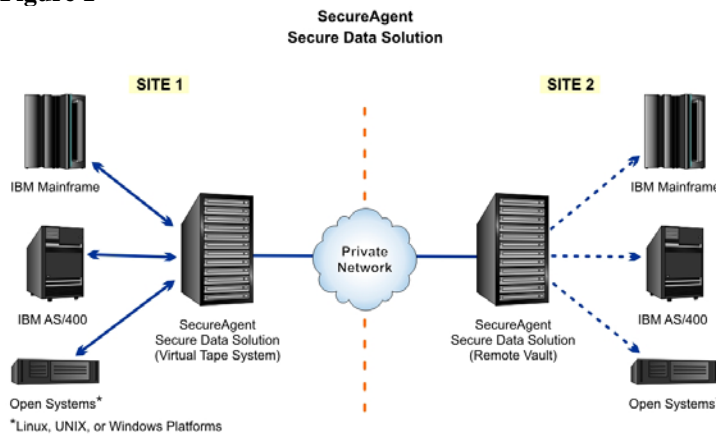
Discussion

The Secure Data Solution®

Virtual Tape System & Remote Vault

The Secure Data Solution (SDS) is a patented and patent-pending virtual tape system and remote vault that allows an organization to efficiently store and retrieve virtual tape images (VTIs). The SDS appears as tape units to attached computer systems; however, in actuality, the virtual tape images are compressed and AES-128 encrypted files that permanently reside on the Secure Data Solution's disk arrays (Figure 1).

Figure 1



As virtual tape images are being written to a local Secure Data Solution, they are also transmitted to another mirrored Secure Data Solution installed at a remote site for disaster recovery or data sharing purposes. Computer systems that are connected to the SDS at these remote sites can immediately share the VTIs. Furthermore, if the virtual tape images are required at more than one remote site,

any number of secondary remote sites can be established for further replication of the same virtual tape images.

Unlike traditional tape, the Secure Data Solution is capable of providing a virtual tape image to be read concurrently by multiple processes (if the operating system allows the same volume serial-numbered tapes to be concurrently read) as soon as a few blocks of the file have been written at either the local or remote sites.

The Secure Data Solution also provides facilities to migrate data from its disk arrays to physical tape at either the local or remote site with attached tape drives, when physical tape is required.

A single SDS can store tape images that have been created by any combination of these supported systems and drives:

- Large-scale IBM mainframes that utilize z/OS or z/VSE and employ the 3480, 3490, 3590, and the even higher speed, higher capacity 3592 tape drives on both ESCON and FICON (including 4 gigabit) channels.
- IBM AS/400s with Fibre Channel SCSI (FC/SCSI)-attached devices that create standard IBM tape labels with volume serial numbers.

- Any Linux®, Unix®, Microsoft®, or other Open Systems platform that utilizes Linear Tape-Open (LTO) or Digital Linear Tape (DLT) tape drives on systems that utilize the IBM® Tivoli® Storage Manager or HP's Data Protector.

Via differently configured Secure Tape Units, a single SDS can store data that has been created by any combination of the above systems and tape drive types.

Unlike physical tapes, the emulated tape devices can be defined to hold substantially more data than a physical cartridge can, reducing the number of multi-volume datasets, and simplifying management of these files. Furthermore, with the Secure Data Solution, precious media is not wasted nor is space reserved—it is dynamically allocated as needed.

Secure Data Solution Components

The Secure Data Solution is an integrated, custom-configured system that is built upon an architecture of non-proprietary, state-of-the-art, computing technology. It incorporates the IDG 9480® or IDG 9483™ Secure Tape Unit™, the IDG 9485® Secure Library Controller, the Virtual Tape Checker™, the Secure Data Mover™, the SA SAN™ Server that manages the attached disk arrays, the IDG 9487™ Secure Tape Controller™, the Secure Agent Administrator™ program, and the IDG 9074® DR Enterprise Operations Console™. The components are interconnected using 1-gigabit, 2-gigabit (dual 1-gigabit), or 10-gigabit Ethernet.

IDG 9480/9483 Secure Tape Unit—Computer systems connect to the Secure Data Solution via an IDG 9480. To a computer system, the IDG 9480 appears as if it is an instance of tape drive controllers and/or tape drives. Each IDG 9480 provides an interface to a computer system and device emulation services, so the computer system believes that it is talking to a native tape drive instead of the SDS. As data is received from a computer system, the IDG 9480 provides compression and encryption (as well as decompression and decryption when reading) services of the data within the virtual tape images, before the data is passed to the SA SAN Server for storage. An organization can define as many tape devices on an IDG 9480 Secure Tape Unit as practical, as long as the interface between the computer system and the SDS provides enough bandwidth to support the number of concurrently used tape drives. When configured with onboard RAID storage, an IDG 9480 is designated as an IDG 9483.

SA SAN Server—The Secure Data Solution's SA SAN Server maintains the tape images on its Raid 5- or the more reliable Raid 6-based disk arrays. Unlike Raid-5, Raid-6 is more robust and can withstand two simultaneous disk failures. There are various configurations to mirror the virtual tape images locally and remotely by the SA SAN Servers or by the Secure Data Mover (described on page 4); these configurations are described on page 4 in SA SAN Configurations. Up to 32 mirrored SA SANs, each capable of managing 32 terabytes of storage, can be installed on a Secure Data Solution's SA SAN Server.

IDG 9485 Secure Library Controller—When virtual tape images are written to the Secure Data Solution's SA SAN, the IDG 9480 not only encrypts the data within the virtual tape images, it also encrypts the file names. Among other control information that is maintained by the Secure Library Controller, it also manages the cross-reference between the actual file names that a computer system knows the VTIs as, and the encrypted file names that the SDS has stored the VTIs on the SA SAN Server. Secure Library Controllers are always locally and remotely duplexed.

Secure Data Mover—The Secure Data Mover transmits virtual tape images to the remote SA SAN over a leased or private IP network. Besides mirrored SA SANs, this is another way to duplex virtual tape images between local and remote Secure Data Solutions. When the Secure Data Mover is used, an IDG 9481® Secure Remote Storage™ unit must be included in the configuration of the remote SDS to interface between the communications link and the SA SAN.

Virtual Tape Checker—The Checker continually ensures that virtual tape images have actually been mirrored. If there had been a problem with the network or a disk array, the Checker will determine what is missing, and will have the Data Mover copy the missing VTIs, or the entire disk array, locally or remotely.

IDG 9487 Secure Tape Controller—The optional IDG 9487 Secure Tape Controller provides connectivity to a fibre channel SCSI-attached IBM TS-xxxx Tape Library or other fibre channel SCSI-attached tape drives when physical tape creation is required. It can be connected to either the local and/or remote Secure Data Solution, depending on where the physical tape creation is required.

SecureAgent Administrator (SAA)—The SecureAgent Administrator provides a single access point across an enterprise that allows an operator to issue commands to all of the Secure Data Solution's components.

IDG 9074 DR Enterprise Operations Console—The optional IDG 9074 DR console provides encrypted TN-3270 remote access to a remote z/OS for console operations. This enables z/OS operations staff to fully operate a z/OS environment remotely.

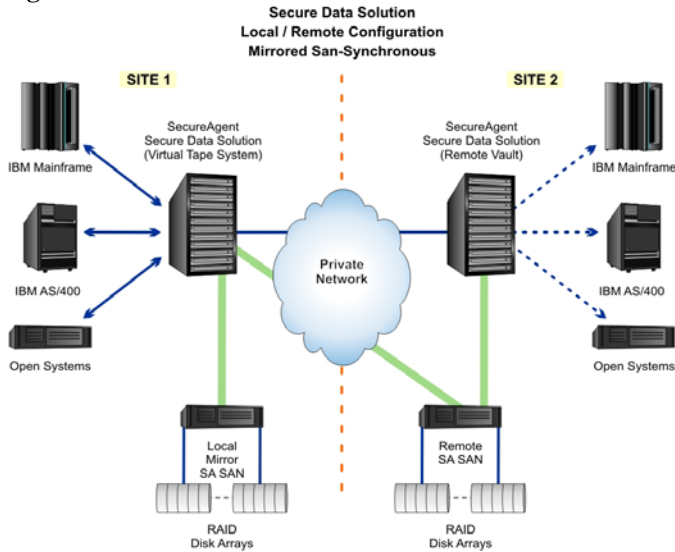
SA SAN Configurations

The Secure Data Solution is available in a number of configurations that can satisfy small, medium or large organizations' needs. The Secure Data Solution's SA SAN Server maintains the tape images on its disk arrays. The possible configurations all have to do with addressing local and remote site data redundancy and connectivity.

Local Mirrored SAN—The Local Mirrored SAN is a fully duplexed SA SAN disk array solution. With the SA SAN, all writes are performed independently to each half of the mirrored SA SAN.

Local/Remote Mirrored SAN—The Local/Remote Mirrored SAN configuration (Figure 2 below) is a mirrored SA SAN; however, the mirror is at a remote location.

Figure 2

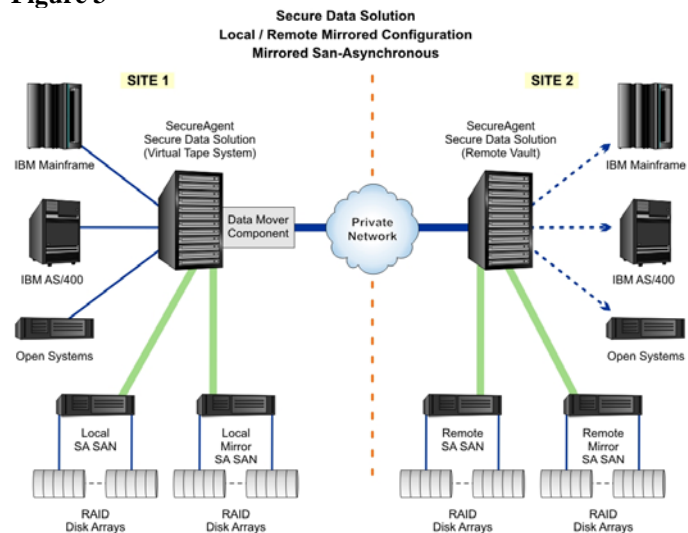


In this configuration, the remote SA SAN is connected to the local Secure Data Solution via a private fibre-attached link and must reside within 100 kilometers. This offers the best in data protection, where one copy of the data resides locally and another copy resides remotely. As with the Local Mirrored SAN, all writes are duplexed and written to both devices independently by the Local/Remote Mirrored SAN. The write is not complete until both acknowledgements are received by the local SA SAN.

Secure Data Mover—For organizations that don't have their own private network, the local Secure Data Solution's Data Mover will transmit the virtual tape images from a local SA SAN Server to the remote Secure Data Solution's SA SAN Server over any private or public IP-based network, regardless of distances or bandwidth (Figure 3).

Unlike the Local/Remote configuration described above, the Secure Data Mover asynchronously copies virtual tape images to a remote SA SAN as bandwidth is available.

Figure 3



SA Host Interface Component

On z/OS and z/VSE platforms resides an integral component of the Secure Data Solution, the SA Host Interface Component. The SA Host Interface Component examines all mount messages and passes the critical information to the SDS regarding the tape being created. It also provides SDS alarms to the OS consoles that can be trapped and addressed by automation.

On z/OS systems, if the remote SDS is connected to another, remote z/OS system, the remote z/OS system's OS catalog and supported tape management system catalogs are updated with the tape information. Supported tape management systems include CA's TMS and TLMS, IBM's RMM, and HP's Data Protector. There are other vendor's tape management systems that Secure Agent is developing an interface to, as well.

Physical Tape

There are times when physical tape is required and the Secure Data Solution provides facilities to migrate virtual tape images to tape at either the local or remote site with tape drives that are attached to the SDS. The physical tape formats that are supported by the SDS include:

- Native IBM 3590.
- IBM TS-1120 format (3592-E05 devices).
- Linear Tape Open (LTO) generations 1 through 4.
- SA Format. The proprietary SA Format creates compressed, stacked, encrypted tapes that can only be read by another Secure Data Solution. Companies that don't have remote configurations and who use a disaster recovery provider who supports SA Format tape transfers can use this facility. The tape transfer process provides a facility that rapidly dumps the entire contents of the local SDS to stacked tapes that can later be rapidly restored at the disaster recovery provider's shared Secure Data Solution. Secure Data Solutions, ready for customer use, have already been installed at a number of major disaster recovery providers' facilities.

Archival Facility

The Secure Data Solution's Archival Facility provides the means to migrate virtual tape images to physical tape at either the Local or Remote SDS. The Archival Facility is offered as an economic alternative to increasing the Secure Data Solution's storage for virtual tape images that have long retention periods and are unlikely to ever be used. The virtual tape images are archived using the SA Format (described above). When a request occurs for a virtual tape image that has been archived, the Secure Data Solution issues a message to the operator to mount the required media on one of its attached drives.

Tape Staging Facility

The Secure Data Solution's Tape Staging Facility provides organizations the capability to rapidly convert from physical tape to virtual tape by dynamically capturing physical tape images. With the tape staging facility, operators load tape drives that are attached to the Secure Data Solution via an IDG 9487™ Secure Tape Controller™, and the entire tape image is captured into the Secure Data Solution's storage. This includes the original volume serial numbers, all the tape labels, and the data from the physical tape. This facility can be used by an organization converting to an SDS, a computing service provider or an outsourcer with new incoming clients, or by disaster recovery providers who have to stage tapes.

Conversion and Use

Introducing the Secure Data Solution into an organization is easy, non-disruptive, and requires minimal changes to an organization's procedures. In most cases the user community is unaware that a conversion from physical tape to the SDS has occurred. However, they do experience an improvement to their processing and wonder, "what changed?"

IBM VTS/ATL Integration/Migration

The Secure Data Solution can be installed and coexist with an existing IBM Virtual Tape System (VTS) and Automated Tape Library (ATL). Furthermore, the SDS can seamlessly migrate virtual or physical tape images from the IBM VTS and/or ATL with minimal disruption to an organization's daily operations.

Scalability

The Secure Data Solution is infinitely scalable. An installation can be initially configured as a stand alone virtual tape system with a few terabytes that supports a few hundred tape images and it can grow into a fully remotely duplexed (or triplexed, quadruplexed, etc.) environment supporting terabytes upon terabytes of virtual tape images. As an organization's tape resource requirements increase, the Secure Data Solution grows with the organization—protecting any prior investment made in the SDS. If greater capacity for tape images is required, then additional storage can easily be added. If more or different tape devices are required, or, more, different, computer systems require connectivity to the Secure Data Solution, additional IDG 9480 Secure Tape Units can easily be added to accommodate the growth. If future, additional remote locations are required, remote units can be installed. The Secure Data Solution is field upgradable, with no planned obsolescence, and growth can be sustained without the need to retire components.

Capacity and Performance

The Secure Data Solution can support up to 2 petabytes of storage. Data compression averages approximately 3 to 1 (which gives an SDS the capacity of maintaining 6 petabytes of raw, uncompressed data).

The Secure Data Solution can be configured to support up to 32 distinctly different tape libraries. There is virtually no limit to the number of unique tape volumes that each tape library can manage—other than what is imposed by the theoretical limit of the six-character volume serial number combination (over 2 billion per library).

The SA SAN Server will load balance the reads and writes across its SA SAN attached disks arrays, to enhance performance. When a virtual tape image is being created, it is written to the least active SA SAN mirrored disk array, and when there are multiple requests to a mirrored SA SAN pair, it will balance the reads of the virtual tape images from either side of the mirrored pairs. Furthermore, the Secure Tape Controller provides indexing information that allows the SA SAN to rapidly locate secondary labels within a virtual tape image for improved performance.

Data transfer between a client computer system and the IDG 9480 Secure Tape Unit is limited by the speed of the attaching ESCON or FICON (4 MB) channels, or by the 4-gigabit FC/SCSI storage network respectively. The IDG 9480's emulation of the IBM 3592 is supported at the 3592's full rated speed. Because of the Secure Data Solution's I/O parallelism, read/write activity across the SAN Server backplane is rated up to 10 gigabits.

Disaster Recovery Testing

The Secure Data Solution provides facilities that allow organizations to perform non-destructive, non-disruptive testing for disaster recovery exercises. At the simulated disaster event moment, half of the remote vault can be disconnected, preserving its contents as of that moment, for a future exercise.

After a disaster recovery test has completed and the remote vault is reconnected, the Secure Data Solution will automatically resynchronize.

Hardware and Software Maintenance and Support

The SecureAgent Service Center (SASC) is available 24 X 7 for questions and hardware or software support. Hardware maintenance meets or exceeds industry standards and is provided by SecureAgent's authorized facilities. The Service Center is capable of remotely diagnosing most issues and can perform software service updates remotely at scheduled intervals.

Summary

A Secure Data Solution normally resides in a standard communications cabinet and requires few environmental resources. An organization can install a remote SDS at another office, a remote data center, a disaster recovery provider, or, their vital records provider's facility. When the remote Secure Data Solution is connected to computer systems at the remote site, the virtual tape images are accessible by the remote computer systems to which it is attached. A single operator console can manage the entire Secure Data Solution environment (all sites).

The Secure Data Solution is a vastly scalable cost-effective alternative to an organization's traditional tape process that saves staff, environmental, off-site tape logistics, and the liability from the loss or theft of sensitive data. It provides more reliable access to data than traditional tapes, improves mount times and tape performance (translating to reduced batch windows), offers rapid access to tape images across multiple locations, and is a solution for disaster recovery.

SecureAgent Software

2448 East 81st Street, Suite 2000
Tulsa, OK 74137-4271 USA

Voice: 918.971.1600

Fax: 918.971.1623

www.SecureAgent.com

The Secure Data Solution is protected by U.S. Patent # 7,293,179; European Patent # 1669872; and others pending.
Secure Data Solution is a registered trademark of SecureAgent Software.