SecureAge

Data Security Solutions

Every File | Every Place | Every Time

Every File | Every Place | Every Time

Protecting information means securing its most common shape and basic element: the data file. SecureAge Technology's take on security does just that. Through the software and hardware products presented herein, SecureAge protects every file throughout its lifespan – from inception to deletion and anywhere else in between – by providing a shield for complete self-defense.

Where Usability Meets Security

It's not enough to merely secure a file. It also has to be accessible and used by those who need it, regardless of their level of expertise and without compromise to their productivity. SecureAge Technology's user-centric, fault-free design across products ensures that there is no trade-off between usability and security. Users and their files are safe whether active or at rest.

A Better Sense of Control

While giving users the freedom to securely produce, create, or even make mistakes, SecureAge Technology's solutions offer administrative oversight and flexibility, allowing for individualized and unique configurations. From granular policy settings to robust log generation, all SecureAge products are scalable for organizations of all sizes, providing limitless control of your data.

Contents

Data Protection Benefits

Protection for Data-at-Rest

While at rest, data is vulnerable against bulk loss or theft either from inside or outside parties. SecureAge Technology has a range of solutions that are designed to protect data stored on any media, in any location, and at all times, either as single files or volumes of collected files.

Inactive or archival data typically outlives the physical hardware and network infrastructure in which it resides. When copied to new media, the data presents issues of replication, secure deletion, and key management problems, leading many administrators to keep the data plain behind periphery solutions. SecureAge solutions allow encrypted data to live forever on any type of media.

Protection for Data-in-Motion

With the majority of data theft and leakages stemming from attacks to data while in use or in motion, SecureAge Technology offers solutions that protect data when in these active states. Data files protected by volume encryption tools only enjoy protection when they are inactive and inaccessible.

Considering data-in-motion to be the most vulnerable, SecureAge products have been developed specifically to maintain the integrity and robustness of the encryption regardless of the state of use or location of any data file. Whether a file is open and active or in transit within an internal network or out on the open internet, SecureAge protects the files in any state, allowing you to work on them safely.

Protection from Malware

Sophisticated malware attacks are launched primarily for the purpose of breaching networks and systems, leaving sensitive information open for exploitation by nefarious parties.

SecureAge tools are not only for preventing data from ever being in a plain or vulnerable state, but also for preventing malware from running in the first place. Application whitelisting can stop unknown processes from executing, while application binding can minimize data loss to a single file type when a trusted application is subject to a zero-day attack.

Deployment Forms

All SecureAge products play a vital role in addressing the entire spectrum of data pathways and rest stops. As such, products are deployed as software on endpoints and servers, and as hardware appliances and servers, including virtual machine and cloud deployment options.

Products and Solutions	Protection for Data-at-Rest	Protection for Data-in-Motion	Protection from Malware	Deployment Forms
SecureData	●	●	●	● ▮
SecureFile	●	●		●
SecureDisk	●	●		●
SecureEmail	●	●		●
SecureAPlus	●	●	●	● ▮
Secure NetGuard		●		▮
LockCube	●			● ▮
Security Management Server	●	●	●	▲ ■
Enterprise SSL VPN	●	●		▲
Data Diode System	●	●	●	● ▮ ▲

LEGEND: ● ENDPOINT SOFTWARE ▮ SERVER SOFTWARE ■ VIRTUAL MACHINE ▲ HARDWARE APPLIANCE

Sales, Services & Support

For use among a variety of customers with a broad spectrum of requirements, SecureAge products are highly customizable and can be configured to meet the needs of any environment of any scale. Similarly, flexible software and hardware purchase plans are complemented by maintenance, support, custom code, and other professional service options.

Licenses

Perpetual and annual license options with tiered volume pricing

Technical Support

Annual or bundles of hours for email, phone, or on-site support

Training

Remote or on-site training for administrators or users

Maintenance

Annual plans for software and hardware updates and upgrades

Consultancy

Pre- or post-purchase consulting on needs and configuration

Customization

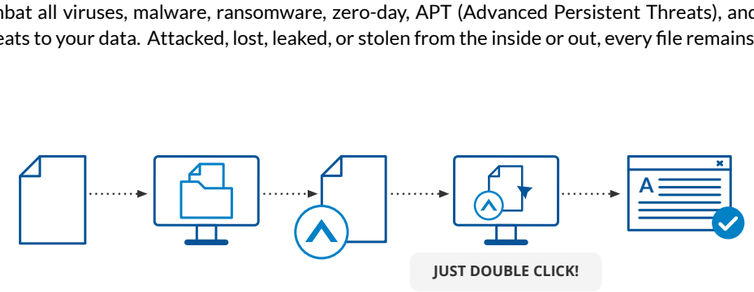
Custom code for unique product modifications or requirements

SecureData

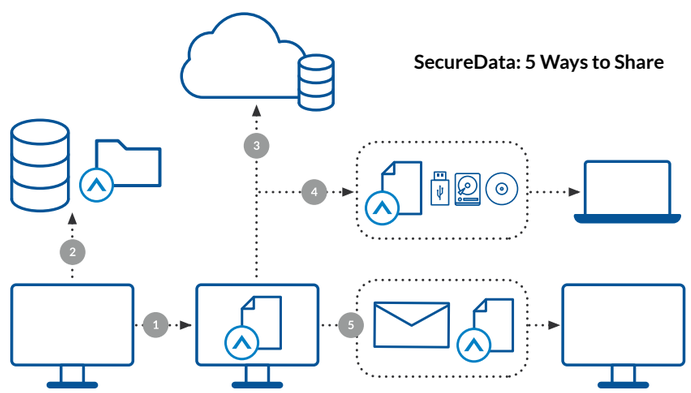
Automatic File & Folder Data Encryption

SecureAge SecureData runs as an invisible endpoint agent that automatically encrypts all user files without user deliberation, action, or even awareness. Employing a seamless PKI implementation, the persistent encryption individualizes and protects each file, whether in use, stored, lost, or stolen.

Moreover, an integrated application whitelisting option and built-in application binding feature combat all viruses, malware, ransomware, zero-day, APT (Advanced Persistent Threats), and other threats to your data. Attacked, lost, leaked, or stolen from the inside or out, every file remains safe.



The individualized encryption of SecureData persists when any file is moved across different storage media, network locations, or, depending on company policy, even when attached to email or stored in the cloud. And using public key infrastructure (PKI), files can be shared for collaboration and access.

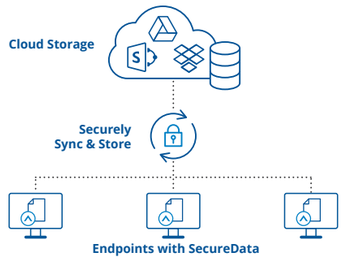


1. Network Transfer (Direct); 2. Shared Network Folder; 3. Shared Cloud Storage; 4. External Media; 5. Email (encrypted email policy)

SecureData

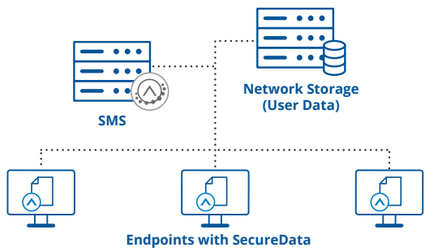
Configurations

SecureData for Cloud Storage / Backup



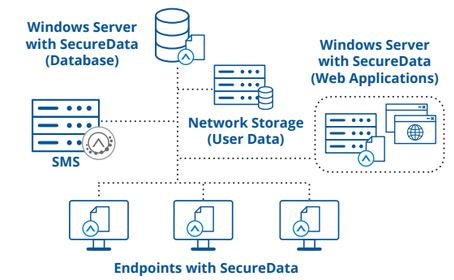
Depending on your preferred usage and configuration, SecureData's automatic file encryption can persist when any file is moved to and stored on commercial or private clouds. The cloud owner or administrator will have no ability to view the contents of the user files protected by SecureData. Moreover, robust log features maintain a clear record of who put what on which cloud, when, where, and in what state.

SecureData for Local Network Storage



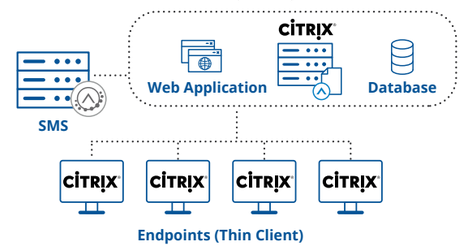
Just as SecureData provides persistent encryption to files stored in the cloud, user files placed on network drives remain both secure and immediately accessible to the file owner. SecureData also allows for the creation of shared folders or entire drives, wherein the files stored may be opened and edited only by those users included on the shared list at any given time.

SecureData for Database and Web Application Server



The same file level encryption of SecureData protects databases, web pages, user data, and any other file type essential for or found on storage servers or Windows production servers. Web applications and related data are safe. And not only are database files secured, but also authenticated queries made to encrypted database files receive the same results without any delay or special processing. Even while encrypted, file content searches remain possible.

SecureData for Thin Client (Citrix)

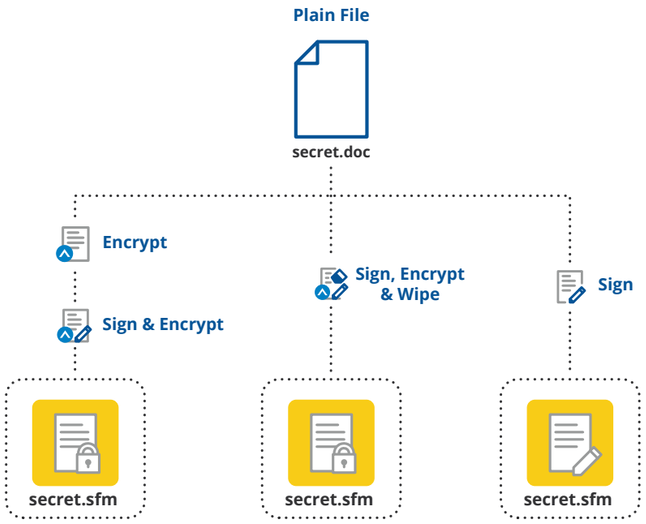


Shared workstations or thin client installations enjoy the same file level encryption and overall data protection that standalone systems do. No matter the number of users or the intent of those sharing workstations, only those files associated with each user's encryption key pairs can be accessed for content viewing or editing. Again, network administrators cannot see file content.

SecureFile

File Encryption & Digital Signing for Mission-Critical Data

Going beyond most file encryption tools, SecureFile provides comprehensive PKI-based document security for select files through encrypting and/or digital signing for compliance or file sharing. SecureFile generates an encrypted or signed copy of a selected file, leaving the original intact.



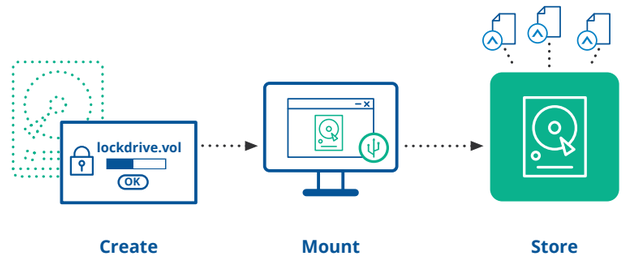
Selected files are protected and file types are hidden to ensure integrity and authenticity when shared by any means with the intended recipient(s). The SecureFile application should exist on both ends.

Most critically, the PKI features of SecureAge allows for the choice of one or more recipients of the SecureFile. From among a list of users for whom public keys exist, the creator of a SecureFile simply selects those to whom a copy of the SecureFile will be shared. Unlike SecureData, which allows for collaboration on a single file in a central location, SecureFile produces local copies for each recipient.

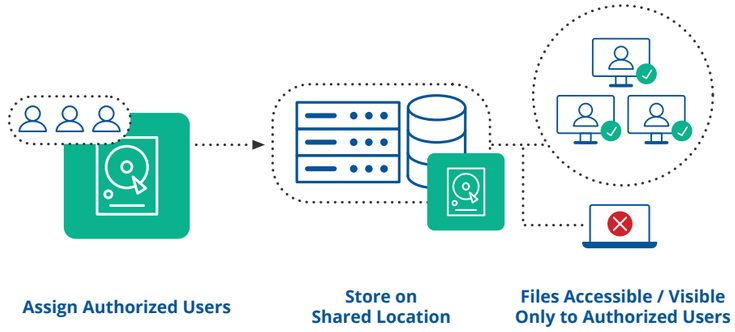
SecureDisk

Volume Encryption to Quickly & Safely Store Confidential Data

SecureDisk creates and manages virtual disk volumes on any Windows-based endpoint or server. All files stored in a single SecureDisk volume are encrypted together and entirely hidden from view. The same benefits of Full Disk Encryption (FDE) or similar come with SecureDisk, as well as the added flexibility of creating one or more volumes at any size chosen by the user and storing it anywhere.



The creation of SecureDisk volumes merely requires deciding upon a size, a name, and a preferred storage location. Once created and mounted, files up to the size limit of the SecureDisk volume can be dragged inside before unmounting, thereafter being invisible and inaccessible to anyone without the key. The volumes may be stored on and retrieved from any media, network drive, or the cloud.



Built upon PKI, SecureDisk offers easy to use and powerful sharing features. Either upon creation or thereafter, the creator of a SecureDisk volume can add other users for shared access, thereby encrypting the contents with the public keys of those authorized users. Placing those shared volumes in a storage location convenient to those users allows for seamless and secure file sharing.

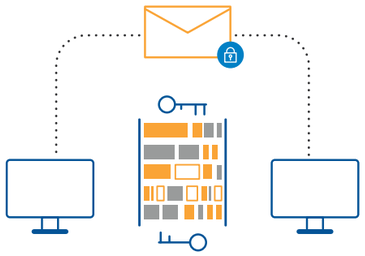
SecureEmail

Policy-based End-to-End Email Encryption

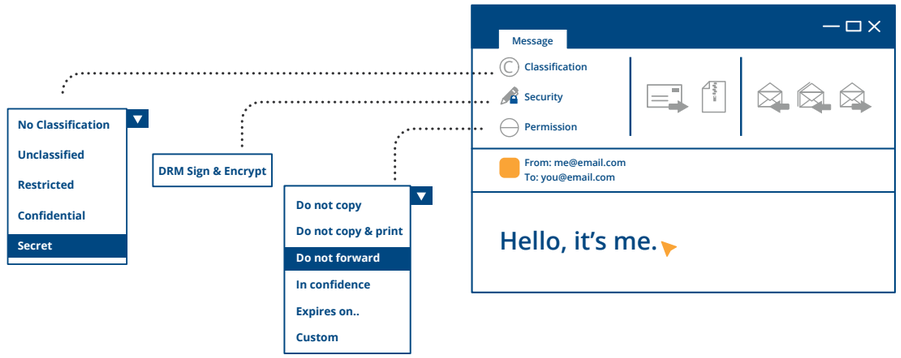
More than enough real-world data breaches have underscored the necessity of encrypting everything, especially email. But the complexities of doing so have been painful enough for most companies and individuals to skip this vital step entirely.

Encrypting email should be as easy as sending email – intuitive and accessible to everyone.

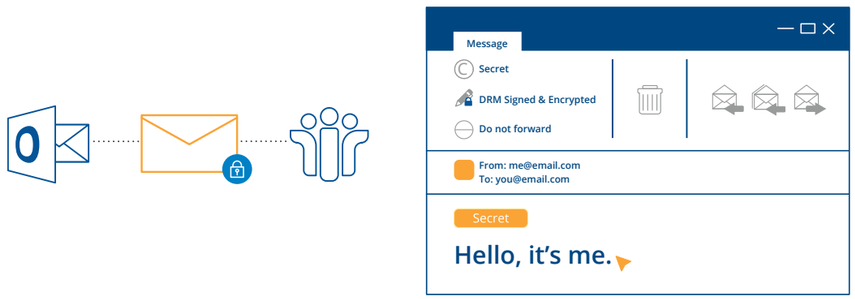
SecureEmail ensures authenticity and privacy without requiring any training or changing the way you send and receive email.



Offering standard PKI features along with unique digital rights management (DRM) options, SecureEmail combines the industry's best encryption technologies for compatibility with invisible, non-intrusive key management.



SecureEmail plugs right into the industry-leading mail client software Microsoft Outlook and IBM Notes, offering drop-down menus for labeling and classifying email. Those user-defined classifications can be linked to security levels, such as sign and encrypt and DRM options that allow for control of messages on the recipient side when both users have SecureEmail.

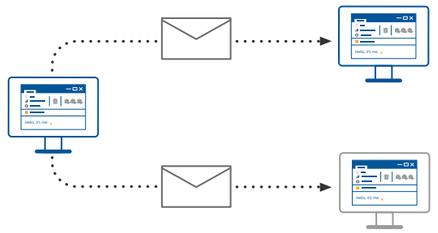


SecureEmail

Send & Receive Scenarios

Sending unencrypted, plain email messages to any email user worldwide remains as easy and familiar as before installing the SecureEmail plugin. Labels such as "Unclassified" or "Normal" can be associated with security levels such as "Plain" or "Unencrypted" per your definitions and settings. On the other hand, unencrypted and plain email can be prevented entirely per user by defining policies that can apply at all times or when either connected or disconnected from a corporate network.

Plain Email: Inside & Outside the Company

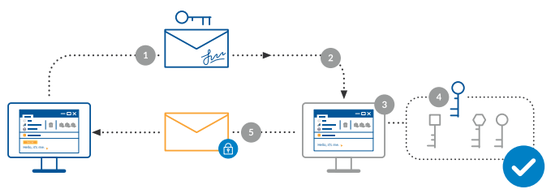


Classification	No Classification
Security	Normal

Encrypted Email: SecureEmail User to SecureEmail User

Classification	Secret
Security	DRM Sign & Encrypt

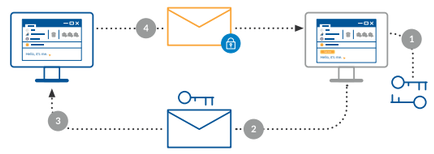
Encrypted Email: SecureEmail User (SE) to Non-SecureEmail User (NSE)



Classification	Secret
Security	Sign & Encrypt

1. SE: Sign email (includes dual usage key)
2. NSE: Import key to Key Manager
3. NSE: Draft a reply
4. NSE: Select proper key for recipient
5. NSE: Send

Scenario 1: SecureEmail user first provides public key to Non-SecureEmail user



Classification	Secret
Security	Sign & Encrypt

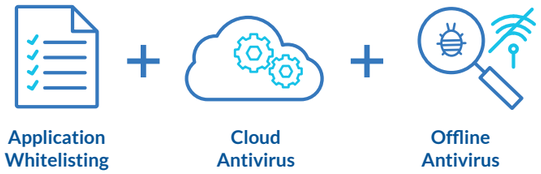
1. NSE: Generate a key pair
2. NSE: Send public key as attachment
3. SE: Automatic import of public key
4. SE: Reply to message

Scenario 2: Non-SecureEmail first user provides public key to SecureEmail user

SecureAPlus

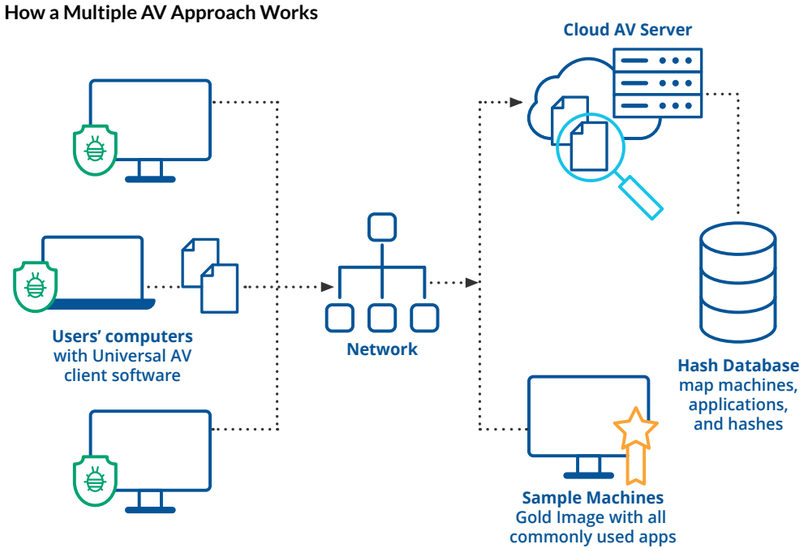
Application Control & Whitelisting with 10+ Cloud Antivirus

SecureAPlus presents a patented solution that's been engineered to protect data from digital threats, such as ransomware or viruses, whether previously known or entirely unknown, going beyond the limits of traditional antivirus products. SecureAPlus's Application Whitelisting stops the unknown.



While previously known threats will be recognized by more than 10 antivirus engines running in the cloud (Universal AV) and by local Offline Antivirus, the entirely unknown threats will be blocked before disruption or damage by the powerful yet simple Application Whitelisting core component. If it's not on the whitelist of approved applications and executables, viruses and malware simply can't run.

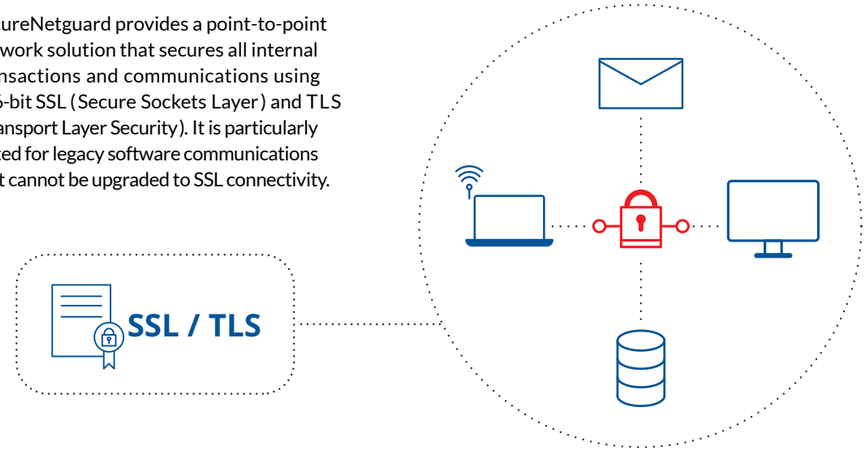
How a Multiple AV Approach Works



SecureNetguard

Point-to-Point Network Security

SecureNetguard provides a point-to-point network solution that secures all internal transactions and communications using 256-bit SSL (Secure Sockets Layer) and TLS (Transport Layer Security). It is particularly suited for legacy software communications that cannot be upgraded to SSL connectivity.

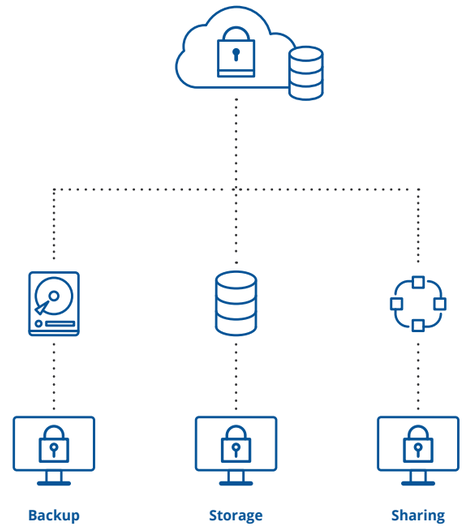


LockCube

Secure & Encrypted Cloud Storage

LockCube offers an encrypted cloud storage service for securely backing up and sharing files (such as Microsoft Office documents, zipped files, pdf, videos, photos and music) across devices. The encryption occurs on the user's machine as files are uploaded, providing security before even reaching the cloud and preventing cloud providers from accessing file content.

Upon download, the files are transparently decrypted and immediately available for use on personal computers or mobile devices in which the appropriate key material has been installed. With the keys invisibly stored on their machines, users experience the convenience of uploads and downloads without a need to manually encrypt or decrypt anything.



The SecureAge Suite

Your Comprehensive Enterprise Security Solution

Comprised of our endpoint software tools, SecureData, SecureFile, SecureDisk, SecureEmail and SecureAPlus, this is our core solution that provides the essential components necessary for complete protection against intentional or accidental data loss or breach from both inside and outside threats.

Deployment requires the mere installation on endpoints and the provisioning of the desired licenses for maintenance updates. A server add-on offers many central management options and benefits.

SecureData provides automatic file and folder encryption for seamless security of all user files without sacrificing productivity or breaking established norms and practices.

SecureFile and **SecureDisk** are tools for particular situations: the manual encryption and signing of files; the creation of volumes that auto-encrypt contents and hide filenames.

The SecureAge Suite is **endpoint license-based,** ensuring maximum flexibility for deployment and scalability to fit the need of any sized organization.

SecureEmail utilizes easy-to-use and user-defined classifications to determine the security of emails. Features include signing, encrypting and DRM options are along with S/MIME for third-party email client compatibility.

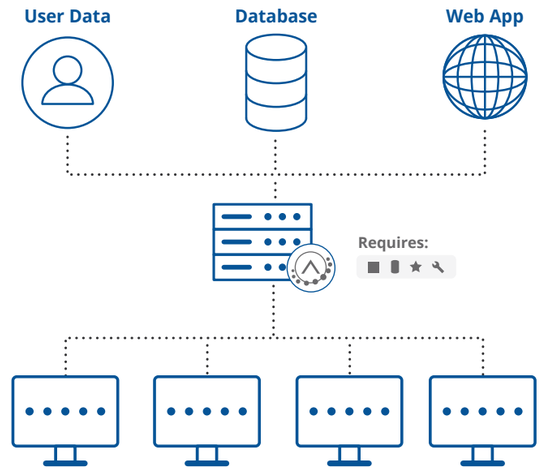
SecureAPlus protects your endpoints against known and unknown threats by creating, maintaining, and enforcing your organization's whitelist locally while using 10+ antivirus engines in the cloud to detect malware.

Security Management Server

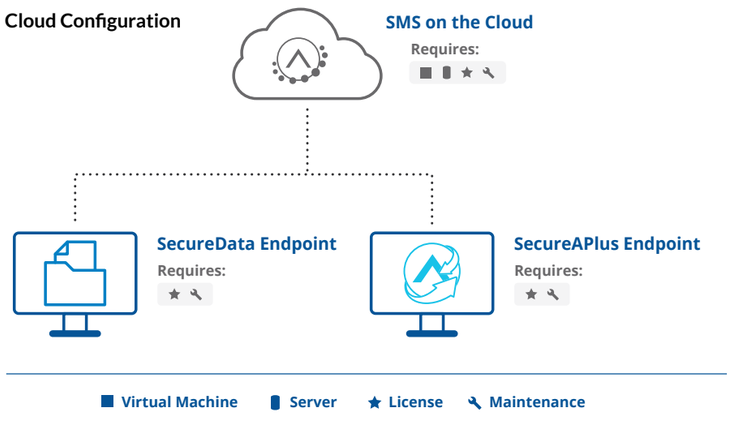
Unified Large-Scale Centralized Security Management

Essential for larger installations, the Security Management Server offers easy creation, distribution, and management of encryption keys, individual user profiles and policies, and software updates to endpoints. It also collects security logs from user machines for total transparency of user activities. It can be delivered either as physical hardware or a virtual machine for various deployment options.

Default Configuration



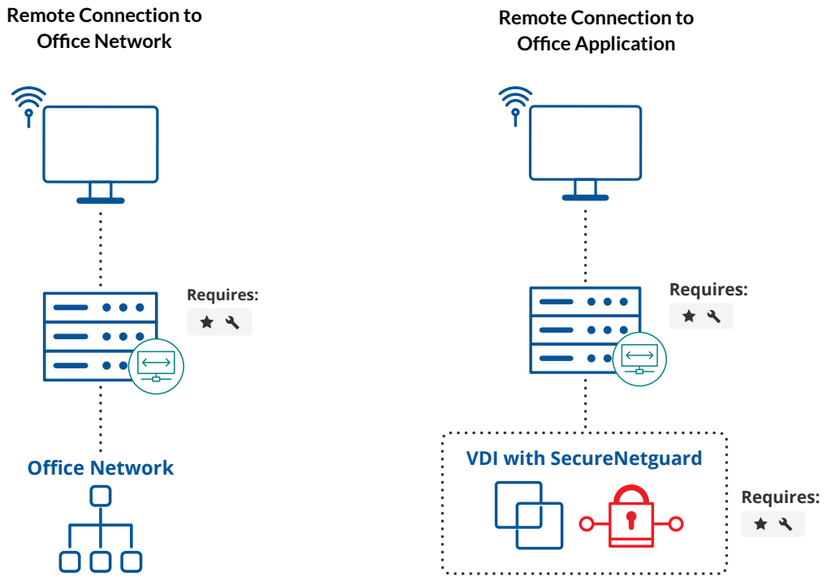
Cloud Configuration



Enterprise SSL VPN

Safe Connections Wherever, Whenever

SecureAge Enterprise SSL VPN is a reliable, easily deployed security solution that allows users to remotely access corporate networks and resources using well-established SSL (Secure Sockets Layer) technology. An IPSec option exists for greater use of devices on either end of the connection.



SSL VPN allows users to securely connect to their network remotely and access services, such as network storage, as if they were physically there.

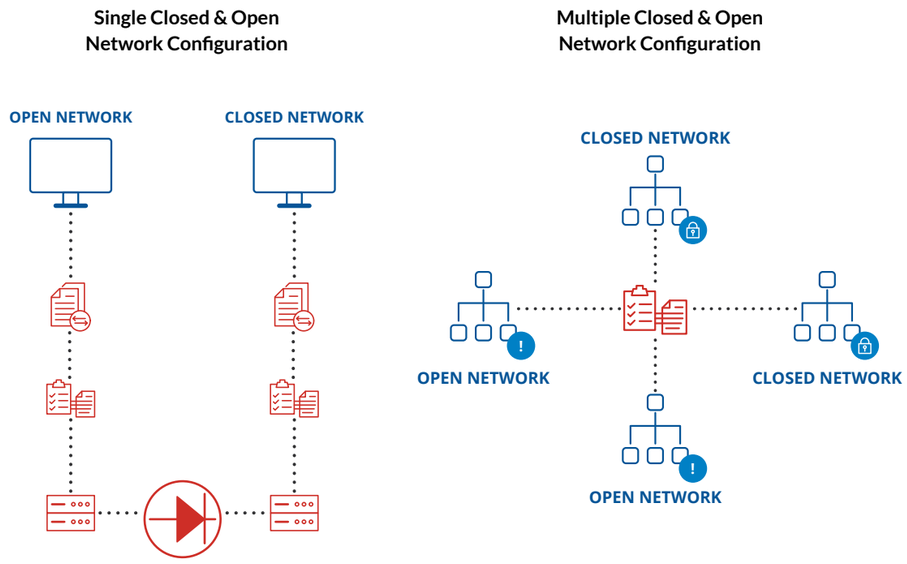
SSL VPN lets users access Citrix or Virtual Desktop Infrastructure (VDI) platforms to allow remote personnel to use office applications and operating systems.

NetGuard is integrated with both SSL VPN servers and remote clients to ensure total security and privacy of data transmission.

Data Diode System

Securely Bridge Air-Gapped Networks

Air-Gapped Security Networks have become popular among organizations that require a strict separation between their secured and unsecured networks. To safely move data between these open (unsecured) networks and closed (secure) networks, SecureAge Technology developed its Data Diode System turnkey solution for rapid deployment to entities of any size.



Closed Network System Core Components

File Transfer System (FTS)

Facilitates the secure handling of files sent across multiple networks. It can be easily accessed through Windows login (single sign-on) authentication or with a dedicated account via local authentication.

Data Diode Proxy

Hardware installed with SecureAge-developed software to ensure total reliability and absolute one-way transmission of data to air-gapped networks.

Information Broker (IB)

Smartly and securely interacting with Data-Diode devices, it encrypts data at rest and in motion for total confidentiality during data transfers. Allowing for the re-transmission of any data not successfully transferred due to data-diode hardware errors, the IB also enables the bridging of multiple open and closed networks.

Endpoint Software

Whether it's a desktop workstation or a laptop, our endpoint protection solutions implement security without sacrificing usability to end-users for maximum and sustained productivity

SecureData
Automatic File and Folder Data Encryption

SecureFile
File Encryption and Digital Signing for Mission Critical Data

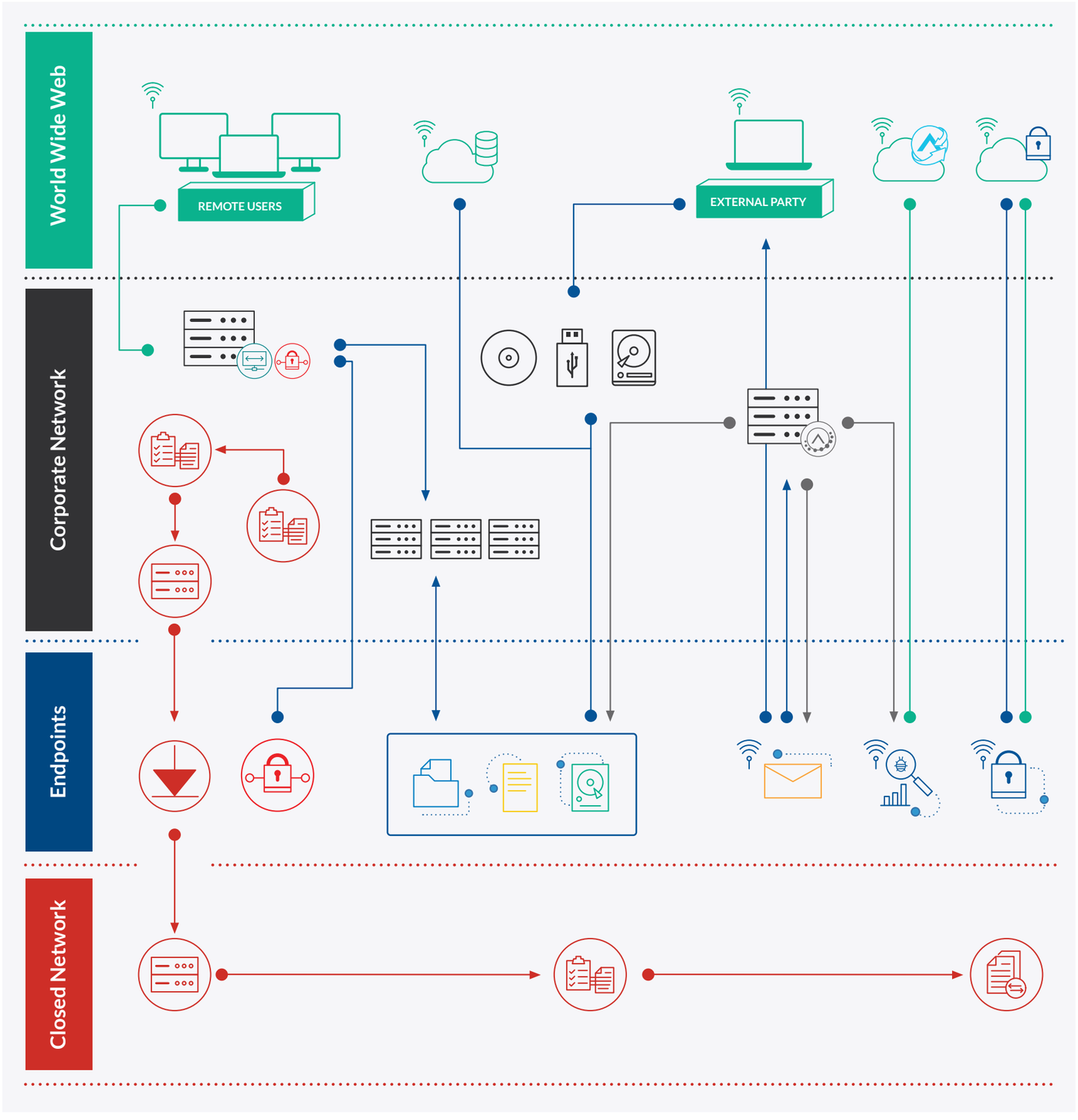
SecureDisk
Volume Encryption to Quickly and Safely Store Confidential Data

SecureEmail
Policy-Based End-to-End Email Encryption

SecureAPlus
Application Control and Whitelisting with 10+ Cloud Antivirus

LockCube
Secure and Encrypted Cloud Storage

SecureAge



Hardware and Network Security

Ranging from software-only to turnkey hardware deployments, our network security solutions are easy to deploy, scale, and maintain leading to stricter security with minimal effort from IT security teams

Security Management Server
Unified Large Scale Centralized Security Management

Enterprise SSL VPN
Safe Connections Wherever and Whenever

SecureNetguard
Point-to-Point Network Security

Data DiodeSystem for Closed Networks

A system that allows the safe transfer of files between a secured and unsecured network without the risk of getting attacked.

The system is composed of the following components:

File Transfer Software (FTS)
Data Transmission Interface

Information Broker (IB)
Efficient and Encrypted File Transfer Management

Data Diode Proxy
One-Way Data Transmission

SecureAge

Our SecureAge representatives are available to advise you on the best security solutions to fit your company's needs. For more information or to schedule a no-obligations demo, please contact us:

SecureAge Technology Pte Ltd. • 3 Fusionopolis Way, #05-21 Symbiosis, Singapore 138633

W www.secureage.com **T** +65 6873 3710 **E** contactus@secureage.com