Overview

Data Leak Prevention Step 1-2-3 ................................................................. 1
SEP Features & Benefits .................................................................................. 3
Secured eDisk Protect ....................................................................................... 5
Secured eUSB ..................................................................................................... 7
Secured eFile ................................................................................................. 9
Secured eMail ............................................................................................. 11
Secured eGuard ............................................................................................ 13
Secured eControl .......................................................................................... 15
Cryptzone’s **Simple Encryption Platform (SEP)** is a centrally managed platform with a modular architecture that offers interoperability, scalability and simple management of a complete data leak prevention solution. SEP provides a proven framework for granular policy-based management of individuals or groups with automated control across multiple applications that protect data in transit, data at rest as well as data in use.

**Data Leak Prevention through Management and Control**

**DLP as easy as 1-2-3**
- Secure portable devices
- Secure data in transfer
- Monitor and secure sensitive information

**Step 1**

**Secure that laptop and USB Memory Stick!**

Securing laptops with hard disk encryption is a straightforward approach that requires little administration as information is automatically written to the hard drive in encrypted format immediately upon hibernation or logging off the computers. The most comprehensive security method to protect desktops and laptops is pre-boot authentication. This method ensures the protection of the operating system, as well as the data files.

Another significant risk is the increased use of devices such as iPods, USB drivers, smart phones and other portable devices. This has lead to a substantial proliferated threat of data leakage and malicious activity on networks. These threats can be mitigated by implementing a port-control solution that prevents the data from being stored on unauthorized devices while balancing usability concerns to ensure continued user productivity.

When protecting data on USB flash drives, administrators should consider policies that require that either the data moved on a USB storage device should be encrypted or the USB memory stick should be encrypted. A simple start up policy could be developed to automatically encrypt all data that is transferred to removable media such as USB sticks or give the user the choice to encrypt the USB stick upon insertion in the computer. It is important to be able to customize policies for individuals, groups of individuals, functional departments and/or facilities to allow movement of sensitive data only to encrypted devices or block the movement by blocking port and/or disallowing external devices.
Step 2
Secure that email & file!

CIOs, CISOs and other professional information security experts must define a security policy that dictates that all data used in transit or moved to a mobile device needs to be encrypted or blocked. For example, a standard security policy would be for all email communication (including the body of the email, subject line and attachments) to be encrypted, if the communication contains sensitive or confidential information. This is especially important when emails that have sensitive information are sent outside the company’s intranet. Another example would be to enforce the encryption of all emails from the Human Resource and Finance Departments if sent internally or externally outside the company’s intranet.

Cryptzone’s award winning Secured eMail enterprise application provides an “easy to use” interface that requires no training for the user and can be deployed in minutes. The Secured eMail solution provides automatic authentication and “encryption key” management of a local basis. The Secured eMail application is an end-to-end solution that allows users to send emails to any user in the world and eliminates the need to exchange complex encryption keys and continuous recipient authentication. With the Secured eMail solution, after the recipient receives the first encrypted email and authenticates the message, the user will never have to input another password – forever! Additionally the Secured eMail solution provides several non-intrusive and very simple ways to read the email.

Files that reside on shared network drives are often exposed to a wide number of users internally. Securing these files with Cryptzone’s Secured eFile encryption based solution allows administrators to define users’ rights and create “secure group access”, as an efficient and straight forward method of access with an extremely high level of security.

Through the power of the Simple Encryption Platform, Secured eFile delivers the ability to secure data for individuals and groups without the need to exchange digital certificates or utilize “phone-based” passwords.

As information rights relationships change, Secured eFile eliminates usability and management barriers to secure file sharing by dynamically enforcing group policies through automated management. The security and access rights travel with the files and folders as users and groups choose to move or copy data from desktops, laptops, servers, USB flash drives, CDs, and external hard drives.

Examples of more complex data patterns:

- social security numbers
- account numbers
- PIN codes
- credit card numbers
- patient IDs
- secure project codes, etc.

When users access “data at rest” - files and folders on networks or shared drives that contain sensitive data need to be encrypted from the moment of creation. Security professionals recognize that users/user groups must be determined in advance to determine access rights to the encrypted data. Typically, files and folders belonging to Finance, Legal, Human Resources and Executive Management are the first to be encrypted.

Step 3
Monitor, find and block sensitive data!

Having completed step 1 and 2, you will have provided a strong foundation for adding more layers of “intelligent” Data Leak Prevention such as data classification and automatic content monitoring and enforcement of your corporate security policy.

Hence, more advanced rules should require the scanning of the content of “data at rest”, “data in use”, and “data in transit” such as an email and all attachments prior to it being sent outside the corporate network. Security policies can be set up to monitor and target information such as social security numbers, credit card numbers, personal information as well as key words such as “confidential”, “classified” and/or actual customer names or other specific words, phrases and/or other expressions.

Depending on the sender and the recipient of the email, the systems will enforce pre-set security rules by automatically blocking the email from being sent, or alternatively encrypt the email in its entirety, before sending it out.

Organizations can gain immediate benefit by deploying a comprehensive data leak prevention system that can monitor and enforce a security policy for all “data at rest”, “data in use” and “data in transit” environments. Administrators can simply set up the security policies and have the system protect against user accidents and malicious leaks of insensitive data.
The Simple Encryption Platform, SEP, provides an organization with the possibility to achieve full DLP through one platform. SEP is a strategic framework that enables an organization to be able to manage all of its data as well as all of its members.

SEP is a centrally managed platform with integrated DLP applications such as encryption, port & device control, content inspection as well as classification of data. This data-centric approach protects data at rest, data in use and data in transit whether the data is located within the network, on the computer or an endpoint device such as a PDA or a USB memory stick.

Key Features

Global Object Synchronization
A Global object is a piece of data that is synchronized between server and clients. The data can be anything from policies, licenses, passwords to templates and enables synchronization for a single user between laptops, desktops and even a Citrix login. This technology makes sure that no matter what computer a user logs into, the user will be able to use the technology they are licensed for, no matter if the user is online or offline.

Global Object Synchronization allows the power of the technology to be the hands of the user, as well as the IT administrator. For the IT administrator - this means that encryption keys, policies, licenses and passwords are always automatically archived for backup. In the case of a computer crash or a regulatory audit, incident logging files and audit reports are close at hand.

Central Management
The Enterprise Server centrally manages and enforces security policies for all Cryptzone products. It has the ability to create custom environments, specific settings and permissions for different groups as well as specific users and then deploy this across an entire network. This managed system allows users to log in to an environment that is appropriate to their needs and consistent from one client to the next.

Role based administration
The platform allows for permissions to be defined for individuals and groups, enabling a flexible multi-tiered administration system with effective delegation of access rights and responsibilities through dedicated user-roles.
Auditing and Reporting
All activities of the managed endpoints are notified in real-time to the SEP server and logged in a database. The events are displayed in the Management Console and communicated to security administrators in a variety of formats such as popup messages and email.

Detailed listing of content reports of lost USB devices, devices used and policy violations on the network and endpoints are also readily available.

System Access Rules and Procedures
Client authentication can be customized depending on the need for user identity verification. From single sign-on (SSO) using Windows authentication, down to authenticating users every time a folder is deleted within a secured area using private passwords. With secured groups, several users can collaborate seamlessly and securely.

License Management
The SEP license management system makes it possible to add, remove and exchange licenses between users, groups and active directories. Licenses can also be issued on a temporary basis to external parties and then withdrawn upon demand. Depending on which license the user profile has included, the client will enable or disable the products dynamically.

Flexible Deployment
The Simple Encryption Platform is designed to be able to run in multiple environments including as a managed service, hosted location and/or in the company’s existing IT infrastructure.

Policy Management
SEP Management Console offers an easy and scalable way to deploy security policies and monitor security to ensure compliance with corporate security policies. Centrally define, enforce and monitor information policies from a single, enterprise-wide console, ensuring a consistent policy across all users in the organization, or customized policies for groups within the organization.

Central Password Management
Synchronizing user profiles to a SEP client also means giving access to secure groups, secure channels and policy settings for passwords, which can be controlled through policies. Users can use Windows® Authentication or their SEP Password to access all encrypted data.

The SEP Management Console will manage user rights and access to secured data using the infrastructure you already invested in – Active Directory.
Secured eDisk Protect offers full hard drive encryption for laptops, workstations, and servers to ensure the ultimate protection against unauthorized disclosure of data and sensitive information.

Today, common threats include the misplacement of mobile devices, theft of PCs, laptops, and servers, as well as data theft when systems are discarded. Organizations need privacy management solutions that ensure sensitive information is protected from unauthorized access as well as eliminate the risks associated with losing mobile storage device.

Key Features

**Transparency & Ease of use**
When IT staff cannot efficiently deploy security solutions, or end users resist adopting security measures, security suffers as surely as if one’s encryption is weak.

Secured eDisk Protect delivers the highest level of usability to minimize application-training requirements. This enables rapid user adoption across the organization, facilitating streamlined deployment.

**Encryption**
Secured eDisk Protect performs low-level encryption, supporting industry proven algorithms such as DES, 3DES, IDEA and AES 128bit, 192bit and 256bit. Users do not notice any impact to their day-to-day activities and are not required to learn or perform anything different. Secured eDisk Protect does not introduce features that requires the user to be trained to operate.

**Pre-boot Authentication**
When a PC secured by Secured eDisk Protect is switched on, the user must first authenticate to the device before gaining access to the operating system and all stored data. If the user is not able to enter a correct username/password, or valid PIN (in the token version), the PC will not boot the operating system and the user will not be able to log into the PC. This ensures hackers cannot break into the operating system to access stored files in the clear.

Users are given three re-tries to enter the correct authentication information. After the third incorrect retry, Secured eDisk Protect will re-start the PC and enforce a one-minute lock out. During this lockout period, the PC will not respond to any user interaction. Once the lockout period is complete the user will be given one single retry to enter the correct credentials. Subsequent one-minute lockouts will occur after each single incorrect retry.
Secured eDisk Protect

Key Features

User Management
Secured eDisk Protect integrates with the Windows user manager to provide seamless user administration and management.

As users are added or removed from Windows, this is automatically synchronized with the Secured eDisk Protect pre-boot authentication screen. Both local and domain user profiles are supported.

Full drive/partial drive encryption
Secured eDisk Protect can encrypt the full disk preventing access to all data, or dedicated sections of the hard drive. At all times, Secured eDisk Protect encrypts all operating system files, including temporary and page files.

Easy Centralized Deployment and Management
Secured eDisk Protect delivers the ultimate ease of administration in networked environments of all sizes. The integration of administration management functionality into Active Directory ensures that administrators work within a familiar management environment.

No training is required for general users to derive the security benefits delivered by Secured eDisk Protect, and only basic administrator training and knowledge is required for deployment and on-going administration. Simple and automated network rollout support, incorporating pre-definable security policies, allows quick and low-cost deployments, even in very large environments.

Pre-boot token support/ Strong authentication
Secured eDisk Protect facilitates increased log-in security utilizing two-factor authentication where smart cards or tokens securely store a private key that is unlocked by the user password. Secured eDisk supports third party solutions like RSA SecurID.

Password Management
User passwords are synchronized with the Windows password, unless this feature is explicitly switched off during installation of Secured eDisk Protect.

Single sign-on
Pre-boot password or token login credentials can be set to automatically be passed on to the Windows post-boot authentication environment, enabling single sign-on to Windows.

Other features
- Transparent encryption with minimal performance loss
- Multi user accounts
- Remote Password Recovery
- Multi-boot support
- X509 certificate support
- Hibernation support
- Integration with User Manager or Active Directory
- Central or Local administration
- Central deployment through MSI

The risk and severity of data theft is increasing due to four predominant factors:

- The increasing value of data stored on computers.
- The increased use of laptops outside the secure network perimeter
- The massive increase in the amount of data being stored
- The progressive efforts and expertise of data hackers and data thieves

These factors, and the growing number of publicized data breaches, are driving more and more rules and regulations concerning data protection and privacy.
Secured eUSB is a software solution that converts and upgrades standard USB flash drives to encrypted and secure USB flash drives with strong central policies.

The storage capacity of USB flash drives have grown tremendously, with costs ever decreasing. The facts of life with most organizations are that employees are using more and more of these devices with or without approval of IT management.

With employees using their own flash drives, traveling with data to customers, and/or taking work home, organizations are constantly at risk from unprotected data on an unsecured flash drive. The consequences can be devastating - lost reputations, lost profits, lost jobs. In short: all the horrors you read about in the daily news.

Key Features

Simple Encryption Platform Ready
Secured eUSB can easily be managed through the powerful SEP Administration Console, empowering the IT Administration to manage licenses, password policies, user rights and to manage and set up secure communication groups through drag and drop experience.

Regulatory Compliance
The Secured eUSB supports and maintains your regulatory compliance efforts. Centralized policy management is automatically enforced for the end user, ensuring that data stored on the device is protected if the USB flash drive is lost or stolen. Your organization can prove that the USB flash drive was encrypted with extensive audit reporting tools. The SEP Management Console can provide detailed content reporting on each USB flash drive, and answer the question for regulatory compliance “what data files were on that lost USB flash drive?”

System access protection
The Secured eUSB solution offers a System access feature protecting access to the secured data. The SEP Management Console can provide custom system access policies to protect the Enterprise network as well as individual users.

Intuitive workflow
The Secured eUSB solution empowers the users to encrypt USB flash drives through a click of a button. The application can be deployed immediately without any level of training. The users can then drag and drop files and folders to encrypt them on the secured USB flash drive. If the user removes the device from the computer it is automatically locked and secured.

Automated Password/Key management
The Secured eUSB solution comes with automated password/key management that eliminates the encryption key headache for both users and IT administrators.
Secured eUSB
Key Features

USB memory stick management and reporting
Deploying and managing USB flash drives can be extremely difficult and complex for an organization. With the SEP management console, IT administrators will have full control over the organization’s secured USB flash drives assets.

Centralized management enables IT administrators with the ability to see what every USB flash drive each user has, when the USB flash drive was created, the last time the USB flash drive was inserted in a corporate computer as well as all of the USB flash drive information such as the vendor and USB flash drive ID. All this data is collected automatically without user or IT Administrators’ involvement. Every user action performed on a Secured eUSB is logged both locally on the USB drive and it is also automatically synchronized to the SEP server.

The SEP Management Console has the ability to create content reports, origination reports and USB flash drive asset reports for every mobility device in the organization. The result is the maximum level of protection over your organization’s assets with a low “total cost of ownership”.

Recovery password
The Secured eUSB solution comes with a helpdesk recovery password feature making it possible for business partners, clients and users to access encrypted USB flash drives even though the password is lost or forgotten.

Security travels with the secured USB flash drive
The security and access rights travel with the Secured eUSB drive. The drive is encrypted with AES256 and the files that are moved to the secure USB drive are automatically wiped from its original location.

Since the security protection travels with the USB flash drives users can create any Microsoft Office file such as Word, Excel and Power Point within the secure working area of the USB flash drive. Users can launch files, make changes and secure them without ever moving the data to an unsecure environment.

Brute force protection
The Secured eUSB solution has a built-in brute force protection system which protects the inherent encryption methodology against professional hackers.

Automatic Data Compression
Data is automatically compressed up to 5 to 1, thereby increasing the current storage of a 1 gig drive to 5 gigs and a 4 gig drive to a 20 gig capacity.

Speed Optimization
The solution actually speeds up data transfers from the computer to the USB memory stick by compressing the data before it is transferred.

Secured Recycle Bin
Every user expects data to be available after it has been deleted. Secured eUSB offers a secured recycle bin located in the secured area of the secured USB. The secured recycle bin travels with the device and the user can restore deleted files located in the recycle bin.

After the Secured eUSB solution has converted a standard USB flash drive, the data on it will be protected with the highest level of security available.

The USB flash drive will have built-in user access control and strong data encryption - ensuring that sensitive data remains secure where ever it travels.

The users can access the secured USB flash drive from any computer by identifying themselves.

Through the power of the Simple Encryption Platform, policies, passwords, licenses, and users are easily managed.
Secured eFile

Protecting intellectual property and customer data are top security concerns for any business today. Whether in transit over a network or at rest on your system, encryption helps secure information, minimizing the risk of being altered or accessed by unauthorized internal and external users.

Secured eFile enables organizations, teams, and information workers to easily share files and folders securely with individuals and groups. Today customers, business partners, and regulators require stronger and more verifiable measures for protecting sensitive information. At the same time, data access is more distributed causing suppliers and partners to become deeply integrated into many organizations’ business processes and IT infrastructures. Continuous sharing of critical data internally and externally creates new security challenges for controlling access to data. Without strong data protection, enterprises may be exposed to significant financial and intellectual property loss, legal penalties, and damage to the brand.

Through the power of the Simple Encryption Platform, Secured eFile delivers the ability to secure data for individuals and groups without the need to exchange certificates or utilize “phone-based” passwords.

As information rights relationships change, Secured eFile eliminates usability and management barriers to secure file sharing by dynamically enforcing group policies through automated management. The security and access rights travel with the files and folders as users and groups choose to move or copy data from desktops, laptops, servers, USB flash drives, CDs, and external hard drives.

The rollout of Secured eFile is a simple process. It perfectly integrates with Microsoft Windows® and existing IT environments. Once deployed, security policies are enforced, and users cannot avoid compliance. Secured eFile helps your organization comply with legislation regarding the security of mission-critical data assets, regardless of where they are moved, shared or stored.

Implementing a security solution is important; however, it is equally important that the individuals whom the organization is communicating with do not feel burdened by the receiving process.

The self-extracting feature enables the organization to send encrypted files to users who do not have Secured eFile installed. The recipient simply double-clicks on the file name and types in the password to access the information.

Key Features

**Simple Encryption Platform integration**
The Secured eFile solution can easily be managed through the powerful SEP Management Console, empowering the IT Administration to manage licenses, policies, user rights and to manage and set up secure communication groups through drag and drop experience.

**Regulatory Compliance**
The Secured eFile supports and maintains your regulatory compliance efforts. Centralized policy management is automatically enforced for the end user, ensuring that data stored in files and folders are protected. Your organization can prove that files and folders were encrypted with extensive audit reporting tools.
Secured eFile
Key Features

Automated Password/Key management
Secured eFile comes with automated password/key management that eliminates the password headache for both users and IT administrators.

Share files and folders on the network
Secured eFile can be used to encrypt files and folders on shared network drives where the access to the file or folder is easily decided by the end user through the secured communication group concept.

System access protection
For enterprises that need an extra layer of security the Secured eFile solution offers a System access feature protecting access to the secured data.

Intuitive workflow
The Secured eFile solution empowers the users to encrypt files and folders through intuitive and easy to use drag-and-drop encryption.

Self-Extracting option
The self-extracting option creates an executable file containing the encrypted content. The recipient of the file simply double clicks on the file name and is then prompted to provide the correct password. The recipient does not need Secured eFile on their computer to decrypt the information.

Recovery password
The Secured eFile solution comes with a recovery password feature making it possible for business partners and clients to open encrypted files if the password is lost or forgotten.

Security travels with files and folders
The security and access rights travel with the files and folders as users and groups choose to move or copy data from shared network paths, FTP servers desktops, laptops, servers, USB flash drives, CDs and external hard drives. A fantastic feature with the Secured eFile solution is that if you do a backup of the secured file or folder it will be secured on the backup itself.

Share and collaborate around secured data
Secured eFile offers the possibility to share and work with encrypted data both internally in your organization and with external parties and customers. Internally it is possible to set up secured groups enabling end users to secure data and then share it on shared network paths, CDs, emails, USB flash drives etc. If a user needs to share data with an external contact there are 3 ways for the external contact to be able to open the encrypted file or folder.

1. The receiver of the data can download a free Secured eFile Reader.
2. The receiver can obtain a license and installation package. This is a good alternative for consistent collaboration. The license can be managed using SEP’s advanced license management system.
3. The third and final way is that it is possible to create self running packages. End users can do this by right hand clicking on an encrypted file or folder and simply choosing to convert to an executable. Then the end user can place the executable on a CD, DVD, USB stick, etc. Secured eFile is one of the few solutions on the market where encrypted data can be opened and read from a CD or DVD.

User logs
All user actions are logged and this is a perfect tool for organizations that have the need to backtrack encryption actions.

Automatic Data Compression
Data is automatically compressed up to 5 to 1, thereby increasing the current storage of a 1 gig drive to 5 gigs and a 4 gig drive to a 20 gig capacity.

Secured Recycle Bin
Every user expects data to be available after it has been deleted. Secured eFile offers a secured recycle bin located in every secured folder. The secured recycle bin travels with the folder and the user can restore deleted files located in the recycle bin. Secured files and folders deleted on the computer will be stored in the standard windows recycle bin secured and can be restored without any problems.

Brute force protection
The Secured eFile solution has a built in brute force protection system which protects the inherent encryption methodology against professional hackers.
Securing data while it travels between colleagues, business partners, suppliers, customers, and other members of an extended enterprise, is crucial. As enterprise networks continue to become increasingly accessible, so do the risks that information will be intercepted or altered in transmission.

As a result of continued high-profile information breaches, corporate enterprises will have strengthened the manner in which they encrypt information as it travels through their network as well as to the networks of their customers, partners and stakeholders.

Cryptzone provides an email encryption solution that combines state-of-the-art encryption technology with ease of use, allowing the use of secured messaging with confidence. Due to the simple process of sending and receiving secured emails, businesses can now use email to communicate and protect their privacy without complex implementation and disrupting users' behavior.

Secured eMail

Key Features

Simple Encryption Platform Ready
The Secured eMail solution can easily be managed through the powerful SEP Management Console, empowering the IT Administration to manage licenses users, groups and policies from one central location.

Eases administrative burden with centralized management
The Secured eMail system, as a part of The Simple Encryption Platform, is managed from one central location.

Full integration with your email client
The Secured eMail client integrates with the email client providing the end user with a new button, "Send secured"
Secured eMail
Key Features

Send to anyone capability
It is possible to create branded receiving instructions with text, graphics and links. Receivers of a secured email are offered a free Reader concept to open secured emails. The free Reader comes in two versions. The first version is a full software Reader offered to receivers where the secured communication will be continuous. The Reader can be integrated into the receivers email client and it will be possible for the receiver to reply back to the sender unlimited. This enables organizations to have a secured communication to external parties without forcing them to purchase a solution.

The second version is a java based reader offered for one-time use and does not demand any installation. The receiver can be a limited user that will be able to open secured emails through a safe sandboxed environment.

System access protection
For enterprises that need an extra layer of security our solution offers a System access feature protecting access to the secured data.

Enforced policy based email encryption
The Secured eControl add on combined with the Secured eMail solution can enforce the encryption action depending on the content of the email and its attachments. The service delivers the protection you need enabling the creation and enforcement of flexible policies matching exact requirements, the service encrypts messages - automatically, instantly, securely - based on sender/recipient information, or detailed scans of email content and attachments for words, names, phrases, numbers and file types.

Complete data confidentiality
The Secured eMail solution protects the email and its content from the sending computer, through the internal network and the internet, all the way to the recipient.

The Secured eMail solution protects the data both inside and outside the enterprise and it is a perfect fit for organizations with outsourced email service.

Automatic Data Compression
All secured emails are automatically compressed up to 5 to 1.

System SKG encryption key technology
The Secured eMail solution is equipped with the latest technology for encryption, AES256. As an addition to that we offer the System SKG technology that increases security and cut IT administration costs that are usually associated with PKI solutions.

User logs
All user actions are logged and this is a perfect tool for organizations that have the need to backtrack encryption actions.

Outbound Content Security - Automated

Secured eControl is an integrated application to Secured eMail. The integrated solution automatically discovers and encrypts sensitive information at desktop level, such as intellectual property, private customer, HR, and financial information, based on content risk policy.

Sensitive information can include personally identifiable information such as Social Security numbers (SSNs) and passwords, custom and pre-defined policies regulations such as for HIPAA, CA SB1386, EU Data Protection Act, Sarbanes Oxley and others.
Device & Port Control

Secured eGuard is our enterprise-grade solution for portable device control that proactively secures your most important corporate information. It controls, monitors and logs how your data is downloaded and uploaded to the endpoints and allows users to create enforceable security policies, view real-time activity and results, and centrally manage any type of removable media, portable storage device and communication interface.

Secured eGuard’s policy-based control of endpoint access to portable storage devices and removable media effectively prevents unauthorized use of enterprise data and enforces endpoint security policies, which comply with regulatory requirements, such as Sarbanes-Oxley, California SB1386 or the Health Insurance Portability and Accountability Act (HIPAA).

Secured eGuard is deployed and managed centrally allowing security administrators to define policies that are automatically distributed to the endpoints using so called Endpoint Agents. These policies are enforced and all relevant events are communicated back to the Management Server.

Close integration with enterprise directories and enterprise management systems enables easy deployment and extensive monitoring and reporting.

Key Features

Advanced Security Agent
The Endpoint Agent is protected from attacks by processes, drivers, services and malicious code on your endpoint. It cannot be bypassed even by users who have administrative privileges to their endpoints.

Management of any device or interface
Secured eGuard can manage internal and external modems, PDAs, iPods, network and local printers, MP3 players, tape devices, biotech devices, CD/DVDs, burners, flash drives (USB flash drives), LAN adapters, camcorders, digital cameras, scanners, optical devices, smart phones, floppy disks, mass storage, SD Cards and zip/jazz drives. Communication Interfaces, such as: USB, WiFi, Bluetooth, PCI, ISA, optical beams, secure digital, PCMCIA, serial (COMs), parallel (LPTs), IrDA and FireWire.
Secured eGuard

Key Features

Live Update Mechanism
The Live Update function controls the software version of the Endpoint Agents. It automatically deploys updates when necessary, minimizing the administrative overhead.

Directory Integration
Endpoint Access Manager is well integrated with enterprise directory infrastructure such as Microsoft Active Directory and Novell eDirectory.

Enterprise Management Systems Integration
Endpoint Access Manager is well integrated with enterprise management systems such as CA Unicenter, CA eTrust and HP OpenView.

Comprehensive Reporter
Endpoint Access Manager records all endpoint I/O events in an SQL database.
A flexible and intuitive reporting module allows administrators to submit customized queries and generate comprehensive reports on endpoint and end user activities.

Intelligent and Granular Policies
Endpoint Access Manager enables authorization of individual USB devices, media and interfaces for specific PCs and users leveraging enterprise directory services.
The information security policies are communicated to the endpoints in real-time and immediately enforced by the Endpoint Agents. Administrators can grant temporary permissions to on-line and mobile users.

Mobile Users Support
Mobile user endpoints are monitored and protected. The Endpoint Agent continues to enforce the policy even when the endpoint is not connected to the network.

Real-Time Notifications and Auditing
All I/O activities of the managed endpoints are notified in real time to the Management Server and logged in a database. The events are displayed in the Management Console and communicated to security administrators in a variety of formats such as popup messages and email. The events are also made available to enterprise management systems in SNMP traps.

Hot-Plug Support
Endpoint Agents monitor Plug-and-Play device drivers that are installed at the endpoint. Based on the policy of that endpoint, the Agent will report the newly installed device to the Management Server and enforce the appropriate access permissions to it.

White and Black List Support of Device
The Endpoint Access Manager allows the creation of policies to either approve specific devices – white list and control the functionality of a device such as approving a specific brand of USB flash drives to be able to have read/write capability and deny –or black list and control the functionality of a device such as allowing the ability to read only and deny the ability to write to the device.
Secured eControl is an integrated information leak prevention solution that protects companies from data loss and information leakage, both inside the organization and the perimeter. Security breaches are increasing in frequency and severity and companies are facing the challenge of protecting their information and under pressure from regulatory and compliance requirements.

The Secured eControl technology adds content aware policy triggering to compliance actions varying from archiving, certified delivery, document rights, and encryption. The integrated solution automatically discovers risk providing the user and the systems administrator with active involvement in risk mitigation which in turn increases policy compliance.

Secured eControl solution delivers outbound content security that enforces information security policies by making employees part of the solution, not the problem. By educating and empowering users about risky data practices, users are aware of the security risks and corporate policies prior to transmitting information.

Increasingly, organizations are at risk to the exposure and loss of sensitive information. Typically, executives have focused on the threat of outside-in attacks on corporate security but insider leakage of confidential information, whether inadvertent or malicious, is grabbing attention due to the financial and legal implications for organizations.

Privacy, intellectual property and financial information should stay controlled inside an organization’s network.

Together with Secured eMail, Secured eControl adds content aware policy triggering to compliance actions varying from archiving, certified delivery, document rights, and encryption.

The integrated solution automatically discovers risk, such as intellectual property and private financial records, hidden legal data information, (metadata) based on corporate policy – providing the user and the systems administrator with active involvement in risk mitigation which in turn increases policy compliance.
Data in Use – eControl client

The **Secured eControl** client is a smart client, which seamlessly integrates with Microsoft Office applications and e-mail clients such as Outlook and Lotus Notes.

The **Secured eControl** client can be configured to alert the user, create an incident report and enforce your security policy actions such as removing the risky contents, converting the data to encrypted file or applying content rights over multiple channels. Rather than only blocking information flow, the **Secured eControl** client warns and educates users in real-time about sensitive information and, if authorized, lets users decide how to treat the content.

**Secured eControl Network Appliance**

Enforce your organizations security and compliance policies with a content protection appliance that unobtrusively monitors content as it traverses or leaves your enterprise network. By deploying the **Secured eControl** Network appliance, your organization can provide a robust last line of audit and control of SMTP and HTTP outbound network traffic.

- Expose and eliminate content leaks and threats through policy-based monitoring
- Gain real-time visibility into policy violations and remediate before being compromised
- Prevent exposure of proprietary or regulated data in email
- Monitor communications to and from mobile devices

The **Secured eControl** Network appliance ships with pre-packed content security policies for private, financial, and intellectual property protection.

**Policy Management**

The system has enhanced real-time assessment and management of risk through integrated policy, alerting, and incident reporting on a client basis.

The Policy Manager provides a centralized point for the distribution of outbound content security policies to either/or and both the eControl client and eControl Network appliance. In addition, the Policy Manager provides centralized audit visibility into content policy violation activity at both end-point and network egress points via reporting.

**Content Filtering & Security**

Alerts notify you when information such as financial data, passwords, intellectual property, customer or employee records are within your email or documents. When implemented within an organization **Secured eControl** can ensure data security and compliance with all of your outbound content security policies.

**Network Monitoring**

Passively monitor, analyze, and process network traffic over HTTP, SMTP, FTP, IM, and Webmail channels to determine if policy violations exist.

**Varied Data Format Discovery**

The system offers analysis of both visible and hidden data in over 370 different file formats, both data at rest and in transit.

**Power Discovery**

The system will discover “data at rest” as well as “data in transit”, to determine if stored data has metadata or other sensitive information that should not be disclosed.

**Document Rights over Email**

Restrict entire documents from being emailed externally or anywhere. Easy to use and requires no IT infrastructure.

**Power User Visibility and Control**

Configurable policy options provide Power User flexibility to override and manage policy-driven content filtering and robust actions such as block, clean risky content, document restriction, PDF conversion and encryption.

**User Transparency**

Automated, policy driven content filtering, cleansing and conversion to PDF of email attachments based on sender, recipient and content, while totally transparent to the user. It is seamlessly integrated with Microsoft Office and automatically enforces company security policy at end-user workstations.

 Rather than simply block information flow, The system warns and educates users in real-time about sensitive information and, if authorized, lets users decide how to treat the content where it be by using encryption, meta data clean, zip, block or use Microsoft Rights Management system.

**Always on Content Risk Alerts**

Alerts identify information that violates privacy, intellectual property and financial disclosure policies.
Satisfied Customers
Awards & Reviews


**West Coast Labs Checkmark:** Email Security

“The Enterprise ePrivacy Suite from Secured Email is a powerful, tried and tested solution that combines ease-of-use and cost effectiveness with proven, user-transparent encryption, to deliver a fresh approach to email security.”


**September 2007**

SC Magazine rates Cryptzone’s Secured eMail Top 3!

“If we had to find one word to sum up this product it would be integration. This product has some very interesting features. Unlike many products of this type, it directly integrates into an email client, such as Microsoft Outlook, and allows the user a choice by providing a “Send secured” button separate from the usual send button. This product also integrates directly with Microsoft Active Directory, which makes user management seamless.”

**EU Awards, Finalists for** - Best Content Security Solution

**SC Awards 2006** - Global Awards, Finalists for: Best Email Security, Best Encryption, Best Security Solution for Healthcare

**EU Awards, Finalists for** - Best Email Security, Best Encryption

**IST Prize 2006**

“Secured eMail has successfully gone through the thorough, highly competitive evaluation procedure resulting in the quality label Nominee for the European IST Prize”