



Getting Started on Protecting Data at Rest

Authors: Daniel Nilsson & Jeff Sherwood

April 18, 2011

Content

Protecting data at rest	3
What is data at rest?	3
Why is protecting data at rest suddenly an issue?	3
Risk assessment checklist	3
What's at risk?	5
Assessing the threats to data at rest.....	5
Regulatory Controls.....	6
The Solution: Encryption with Strong Authentication	7
What is Data Encryption?	7
How Encryption Can Be Applied	8
Strong Authentication for Access Control.....	10
Encryption requirements checklist	11
Cryptzone's solution for data at rest protection	11
Conclusion	12
About Cryptzone	13

Protecting data at rest

What is data at rest?

Data at Rest is any data that resides on your laptops, desktops, even your mobile devices, such as Personal Digital Assistants (PDA) or Flash Drives. This data can be in the form of documents, spreadsheets, database files, or any other file generated by an application that you use. While active and relevant, this data is not in a state of transmission and is, therefore, called Data at Rest. However, because of the pervasiveness of devices such as laptops, PDAs, etc., even though the data is at rest, the device on which it is stored is in a state of motion, effectively exposing the data to all types of security risks.

Why is protecting data at rest suddenly an issue?

For any company, looking inward at the state of its data security can be an eye-opening experience. Many organizations find that they are vulnerable in ways they had never even considered. In many instances, an organization is not even cognizant, to any degree of specificity, of where sensitive information resides within the network and who has access to it.

In today's world, data no longer exists solely within the confines of a network server room, accessed only between business hours when an employee is physically in the office at their computer. Those days are long gone, and, most likely, never to be seen again. Through ever-evolving technology, business is now able to be conducted at anytime from anywhere. But this convenience does come with some inherent risks.

In current business environments, not only does sensitive data reside on various servers and workstations throughout an organization, it has become pervasively transportable through the use of laptops and removable media devices, such as flash drives, memory cards, CDs, and external hard drives. Protecting sensitive data, no matter where it resides, and ensuring that only the appropriate persons have access to that data, must be a core requirement of every company's data security strategy.

The challenge in achieving data privacy is to protect data, while allowing the data to be shared. With the rising incidence of threats to sensitive data, and increasing requirements by governments and other agencies to protect that data, organizations must focus squarely on their security infrastructure. It is imperative that organizations implement security solutions that will not only protect important data assets, but also satisfy growing regional, national, and global data privacy and security regulations.

Prior to implementation of a security plan, an organization must first perform a comprehensive analysis of their data security needs. This "self-examination" should be done from the top down, encompassing all departments and data access scenarios. It is imperative that security needs be identified prior to implementation so that specific needs of privacy and compliance can be met.

Risk assessment checklist

To help determine the current state of data security practices, and establish where changes need to occur, Cryptzone has developed the following Risk Assessment Checklist. Most of these questions are very basic, but are ones that many organizations don't think about, or, if they do, put off implementing the necessary protection due to budgetary constraints or manpower. But for organizations that are not currently protecting their data at rest, the more important question is "can one afford not protect the privacy of one's data?" Account and transaction information, customer listings, employee and patient profiles, intellectual property—these are all critical business' assets and their security is essential to the operation, continuity, and ultimately the success, of the organization.

The challenge in achieving data privacy is to protect data, while allowing the data to be shared.



QUESTIONS	YES	NO
Are employees allowed to work remotely?		
Do employees travel frequently?		
Are laptops provided to employees for company purposes?		
Is the use of removable media for file transfer allowed?		
Is firewall, anti-virus, and/or anti-spyware software active and up to-date on all workstations?		
Is your organization required to comply with specific government mandates or data privacy regulations?		
Does your organization have a defined, comprehensive security policy, including security practices, operating procedures, and user roles and responsibilities?		
If you answered Yes to the previous item, are all employees trained on the security policies and procedures?		
Is protecting sensitive data at rest a current or planned priority for your organization?		
If a data storage device (laptop, desktop, flash drive, etc.) was lost or stolen, would you be able to efficiently determine if the device contained sensitive or confidential information?		
Is there a standard procedure in place for responding to the loss or theft of a data storage device?		

With mounting regulatory considerations and an overall focus on securing data, it is more important than ever to design and implement a comprehensive plan of protection to provide not only the enterprise, but their employees, associates, and customers with the assurance that their data is completely secure at all times.

What's at risk?

Data protection is important to anyone who works with and stores data, encompassing a broad range of industries—financial services, government, medical, educational, insurance—just to name a few. Security breaches can have a far-reaching impact to not only a company's finances, but to their reputation as well. For government agencies in particular, it may even be a matter of national security. The types of data at risk include intellectual property, corporate financial information, internal communications, customer and consumer data, and employee information.

There is an expectation from customers, employees, and partners—anyone who entrusts a company with their sensitive data—that this information is protected. Organizations must consider all of the potential damage that can be done to their business if sensitive data is lost or stolen—lawsuits, negative publicity, loss of sales and customer confidence, and permanently tarnished reputations.

Ask yourself one simple question - if your laptop was lost or stolen, would the data stored on its hard drive be at risk? If it is currently protected with no more than a password, the answer is yes. And, unfortunately, this would most likely be the answer for the majority of users. Today, the risk extends well beyond the traditional network perimeter to employee and contractor laptops, and other portable storage devices, as the global workforce becomes increasingly mobile. In the last year alone, there have been scores of reports of lost or stolen laptops that contained sensitive data. This, combined with inadequate security policies and lack of oversight, place companies in a very tenuous situation.

Assessing the threats to data at rest

In July 2010, the Digital Forensics Association, published a study, tracking data breaches and thefts, reported that the number of data records exposed to threat reached 721 million from 2005 to 2009, which is over two years ago.

This statistic is even more troubling due to the fact that Privacy Rights Clearinghouse (PRC) is a nonprofit consumer organization with a two-part mission – consumer information and customer advocacy, has reported that the trend is escalating in a hockey stick mode, whereas data breaches are routinely reported daily in the newspaper and viral across the Internet.

According to this group, the greatest risk of exposure comes from employees or consultants who do not properly secure the data they are entrusted with. Whether through neglect or misfortune, these incidents continue to increase at an alarming rate. In the last year alone, there have been scores of reports of lost or stolen laptops that contained sensitive information. Combined with the continuing risk of intrusions from hackers intent on theft or sabotage, any organization that fails to implement a comprehensive data protection plan is simply adding to the already present risk. Here are just a few examples of recent incidents:

- **Health Net Inc.** - In March 2011, nine data servers that contained sensitive health information went missing from Health Net's data center in Rancho Cordova, California. The servers contained the personal information of 1.9 million current and former policyholders, compromising their names, addresses, health information, Social Security numbers and financial information.
- **Ortho Montana** - In March 2011, a laptop was lost or stolen that contained information relating to 37,000 current or past patients.
- **Saint Francis Broken Arrow Medical Center** - In February 2011, a computer that had not been used since May of 2004 was stolen from a secured information systems room. The information would have included names, Social Security numbers, dates of birth, addresses and patient insurance and diagnostic information of 84,000 names of patients and employees.
- **Department of Corrections, Oregon** - In February 2011, an outsider with a thumb drive that contained confidential payroll information contacted the agency on January 27. The thumb drive contained payroll reports with the information of around 550 staff members. Pay stub data with names, Social Security numbers and other payroll information were exposed.

- **Friendship Center Dental Office, Florida** – January 29, 2011 a laptop computer was stolen containing protected health information of 2,200 individuals.
- **Warner Pacific College, Oregon** - In January 201, a laptop was stolen from an employee's home on January 3. It contained the names, Social Security numbers, date's of birth, telephone numbers and addresses of 1,536 students.

While these examples represent a very small percentage of reported incidents, but mostly important these are just within the last few months and they serve to illustrate just what is at risk for both the professional organization and the private citizen. With mounting regulatory considerations and an overall focus on securing data, it is more important than ever for organizations to design and implement a comprehensive plan of protection to provide not only the enterprise, but their employees, associates, and customers with the assurance that their data is secure.

In July 2010... the number of data records exposed to threat reached 721 million.

Regulatory Controls

Regulations have been implemented by state and federal governments, as well as other agencies, to ensure the protection and privacy of sensitive data. Many organizations must comply with a variety of regional, national, and international directives. Here's a list of several major regulations currently in place:

Examples of Current Data Protection Regulations	
Regional	<ul style="list-style-type: none"> • California Database Security Breach Act (SB 1386) • Washington Substitute Senate Bill No. 6043 (SB 6043) • New York Information Security Breach and Notification Act (A04254) • Massachusetts 201 – CMR 17.00 • Nevada SB 227 - 38 more State rules and regulations
National	<p>United States</p> <ul style="list-style-type: none"> • Federal Information Security Management Act (FISMA) • Gramm-Leach-Bliley Act (GLBA) • Health Insurance Portability and Accountability Act (HIPAA) • HIPAA Hitech Act • Sarbanes-Oxley (SOX) <p>Japan</p> <ul style="list-style-type: none"> • Personal Information Protection Act • J-SOX <p>Other</p> <ul style="list-style-type: none"> • Hong Kong SAR China Personal Data Ordinance • Taiwan Computer-Processed Personal Data Protection Law • New Zealand Privacy Act • Canada Personal Information Protection Electronic Doc Act
Global	<ul style="list-style-type: none"> • EU Data Protection Directive 5/46/EC • Basel II • Payment Card Industry Data Security Standard (PCI DSS)

Penalties resulting from a failure to comply with applicable regulations can include fines, Heightened scrutiny, exclusion from programs, credit downgrading legal prosecution, and, possibly imprisonment.

Penalties resulting from a failure to comply with applicable regulations can include fines, heightened scrutiny, exclusion from programs, credit downgrading, legal prosecution, and, possibly, imprisonment. In the case of ChoicePoint, mentioned in the previous section, a settlement was reached with the Federal Trade Commission for \$10 million in civil penalties and \$5 million for consumer reparation, allowing victims of identity theft due to the data breach to be reimbursed for out-of-pocket expenses. Under the proposed Personal Data Privacy and Security Act of 2005 (U.S. Senate, Specter/Leahy), businesses that fail to implement adequate data protection practices could be fined up to \$500,000 per violation.

The Solution: Encryption with Strong Authentication

It is a proven fact that only encryption can protect data no matter where it is stored, ensuring that the confidentiality and integrity of that data is achieved, and allowing organizations to meet regulations for protecting the privacy and security of shared information.

The use of encryption as the basis of any data protection strategy provides a simple solution to many security challenges, allowing an enterprise to create a plan that provides complete data protection with a one-to-many effect. Encrypting data at rest is vital so that only authorized individuals can view and manipulate that data. If a person or process fails to prove identity or is not authenticated, access to the data is denied. The data remains confidential and the integrity of that data is achieved. And, because of its performance, ease of implementation and management, depth of security, and cost-effectiveness, encryption is an optimal solution for securing an organization's data at rest, and for addressing government and industry requirements for compliance and confidentiality.

What is Data Encryption?

Encryption is a secure process by which data is "scrambled" using a key algorithm (a.k.a., secret code), rendering it unreadable. Only authorized users who have the key will be able to decrypt and read the data. Encrypted data is typically referred to as cipher text, while unencrypted data is called plain text.



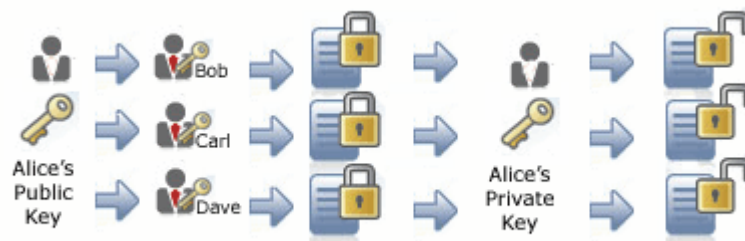
Encryption is based on the science of cryptography, with most computer encryption systems belonging to one of two categories - symmetric encryption and asymmetric encryption.

- With **symmetric** encryption, each computer has a private key (code) that is used to encrypt a packet of data before it is sent over the network to another computer. This type of encryption requires that you identify which computers will be talking to each other so that the private key can be installed on each one, allowing the sender to encrypt the data and the receiver to decrypt the data.



The use of encryption as the basis of any data protection Strategy provides a simple solution to many security challenges...

- Asymmetric** encryption (also known as public key encryption) uses both a public key, which is known to everyone, and a private key, which is known only to the recipient of the data. The private key cannot be determined from the public key. For example, Alice generates a pair of keys and tells everyone her public key. Anyone can use Alice's public key to send her an encrypted message, but only Alice knows the private key to decrypt it. This allows Alice to communicate in private with anyone that has her public key, since only she has the key to decrypt each message.



Encryption offers the best possible protection for data at rest, ensuring that The confidentiality and integrity of that data is achieved, and allowing organizations to meet government regulations for protecting the privacy and security of shared information.

There are several variants of encryption technology, one of the most popular being the Data Encryption Standard (DES), developed in the mid-1970s by IBM. DES is a method of cipher (numerical encoding) used to encrypt data. DES was quickly adopted by the U.S. Department of Defense, and its use soon spread among government agencies, becoming an official Federal Information Processing Standard (FIPS). Eventually, the use of DES moved into the public domain. Over time, more secure forms of DES were developed — 2DES and 3DES — which are simply successive invocations of the standard DES algorithm, providing increased key strength.

In recent years, the DES variants have been superseded by the Advanced Encryption Standard (AES), a block cipher that supports a larger range of key sizes (128 up to 256). AES, like DES, has been designated an encryption standard by the U.S. government, and has been accepted extensively worldwide.

Encryption is now widely used to protect all types of data systems, such as corporate networks, Internet e-commerce transactions, bank ATMs, and mobile phone networks. Encryption offers the best possible protection for data at rest, ensuring that the confidentiality and integrity of that data is achieved, and allowing organizations to meet government regulations for protecting the privacy and security of shared information.

How Encryption Can Be Applied

To achieve the highest level of protection, Cryptzone advocates a “layered” approach—four separate layers of protection that work together to provide a complete strategy, ensuring that data remains secure in any circumstance. On its own, each layer of encryption is effective, but cannot cover every eventuality. However, by encrypting data at multiple layers, an organization maximizes the effectiveness of its security, no matter whose hands a lost, stolen, or recycled laptop ends up in. Let's take a closer look at each layer:

...by encrypting data at Multiple layers, an Organization maximizes the effectiveness of its security, no matter whose hands a lost, stolen, or recycled laptop ends up in.

- **Full Disk Encryption** (Power off Protection) encrypts the entire hard drive (including operating system files) of a laptop or workstation to protect against disclosure of information in the case of theft or accidental loss of the hardware device, or re-use after being sold or leased. Full disk encryption protects all of the data contained on your drives and should be viewed as a logical first step as a company embarks upon its mission of implementing data at rest protection. Major benefits include:
 - Encrypting operating system files ensures that an unauthorized user cannot manipulate these files into a "Safe Mode" and gain access to the data resident on the hard drive. This is further strengthened by requiring the user to be authenticated before the operating system files are loaded into the memory of the computer.
 - There are no selective or hierarchical privileges associated with this level of encryption; access is an "all or nothing" scenario.
 - Many data breach regulations (such as California SB 1386) state that notification of loss or theft of a data storage device is not required if full disk encryption was used on the device.
- **File/Folder Encryption** (Power on Protection) allows encryption of individual files and folders stored on servers, workstations, laptops, and portable media that contain confidential information. As long as the computer is not powered on, the full disk encryption is effectively protecting all data on the drive. However, upon boot-up and proper authentication, the full disk encryption allows access to the entire drive.

What happens if you walk away from your desk and leave your desktop unlocked? Can one of your colleagues "inadvertently" walk over and "borrow" one of your files? While we absolutely trust our colleagues, the truth is that a good percentage of data abuse is attributed to company employees! It then becomes imperative that we put in place a control to ensure that the "power off" protection is also extended to the "power on" state. And this is where the file/folder level encryption comes into play.

By encrypting individual files and folders stored on servers, workstations, laptops, and portable media, the file/folder encryption makes sure that sensitive data is always in an encrypted form and is not "inadvertently" shared with unauthorized users. In addition to allowing encryption of files and folders on your own machine, the file/folder encryption allows the encryption of shared folders, access to which can be managed locally or through a central location; the choice, of course, is dictated by the company's security policies. This then becomes the second level of data at rest protection.

- **Database Encryption:** With the hard drive and the files/folders encrypted, you have successfully mitigated the risks associated with exposure of data either from a stolen/lost asset or inadvertent/malicious extraction of files from a machine. Now you start focusing on securing your databases. By encrypting data that you have identified as critical or sensitive, and limiting its access to users whose job requirements necessitate access to this data, you are able to maintain the integrity of your database and ensure that the data is not vulnerable to unauthorized access. In addition, you have an audit trail that assists you with forensics.
- **Application Encryption** enables you to encrypt various data fields, and ties in data access to user privileges. Application encryption provides granular access control to your applications, allowing them to stay secure. Only authorized users would have access to encrypted fields, once again limiting access to the appropriate users. Much like database encryption, application encryption provides you with an audit trail, allowing you to quickly track down the perpetrator in case of a violation.

The ability to encrypt data so that the loss of that data becomes a near impossibility is unquestionably the greatest return on investment an organization can have.

...by encrypting data at Multiple layers, an Organization maximizes the effectiveness of its security, no matter whose hands a lost, stolen, or recycled laptop ends up in.



	Does	Benefits
Application Encryption	Encrypts Applications	Protects Application data by limiting access only to authorized users (can be based upon job coded)
	Provides granular protection for applications	
Database Encryption	Encrypts Databases	Maintains database integrity and limits access only to authorized users whose job requirements warrant it.
	Provides granular protection for databases	
File/Folder Encryption	Provides Power On Protection	Assures that somebody cannot compromise security of sensitive data by "inadvertently" gaining access to certain folders
	Encrypts individual files & folders	
Full Disk Encryption	Provides Power Off Protection	Assures that data is secure even in case of theft or lost asset
	Encrypts the entire hard drive including operating system files	

The ability to encrypt data so that the loss of that data becomes a near impossibility is unquestionably the greatest return on investment an organization can have.

It is vital that an organization achieve the highest possible level of assurance that data inside and outside of the network perimeter is protected. By applying encryption at multiple levels, the defense against data loss is substantially fortified. The ability to encrypt data so that the loss of that data becomes a near impossibility is unquestionably the greatest return on investment an organization can have.

Strong Authentication for Access Control

Authentication is, in very basic terms, the act of confirming that someone (or something) is who (or what) they say they are. To do so in a secure fashion, one or more "authentication factors" are used to prove identity. The most commonly used factors are:

- Something you know – password or PIN
- Something you have – smart card or USB token
- Something you are – biometrics, such as fingerprint, retina, signature, voice

The use of two-factor authentication, also referred to as "strong" authentication, is becoming increasingly widespread as organizations look to strengthen traditional password-based systems. The most common form factor to complement password authentication on desktop and laptop computers is a smart card or USB token, given their diminutive size and affordability. In this case, authentication is enforced through insertion of a smart card or token along with a password or PIN in order for the user to gain access to the local computer's hard drive and the corporate network.

Taken a step further, "pre-boot authentication" can be implemented to require user validation before the computer's boot process is even allowed to begin. This prevents unauthorized access not only to stored data, but also to the operating system files, eliminating the possibility of hackers accessing the hard drive.

When encryption is implemented in conjunction with a strong authentication process, an organization can rest assured that their information assets are safe, that its security practices are compliant, and that the company's reputation and brand equity will be protected.

When encryption is implemented in conjunction with a strong authentication process, an organization can rest assured that their information assets are safe, that its security practices are compliant, and that the company's reputation and brand equity will be protected.

As with other seasoned forms of information security, the level of security has a direct and positive correlation to the granularity of the implementation.

Encryption requirements checklist

Cryptzone has developed the following checklist to be used as a guideline when selecting encryption and authentication solutions for your data security plan. The items listed in the checklist are the minimum functions that an encryption product should provide to ensure complete protection against unauthorized access to sensitive data. Any product that does not meet these minimum requirements should not be considered.

X	REQUIREMENT
	Full disk encryption with pre-boot authentication to protect data in the event of storage device loss, theft, or reuse
	<ul style="list-style-type: none"> • Encryption process should be transparent to end-user
	<ul style="list-style-type: none"> • Two-factor pre-boot authentication with token or smart card
	<ul style="list-style-type: none"> • Ability to encrypt removable media storage devices
	<ul style="list-style-type: none"> • Allows centralized or local management of users
	<ul style="list-style-type: none"> • Supports boot into multiple operating systems on a single device
	<ul style="list-style-type: none"> • Interoperable with existing applications
	<ul style="list-style-type: none"> • Single Sign-On capability
	<ul style="list-style-type: none"> • FIPS140-2 and Common Criteria compliant
	File/folder encryption to protect individual files and folders
	<ul style="list-style-type: none"> • Encryption process should be transparent to end-user
	<ul style="list-style-type: none"> • Ability to control role-based access rights within user groups to encrypted files and folders
	<ul style="list-style-type: none"> • Automatic authentication and key management
	<ul style="list-style-type: none"> • Single sign-on
	<ul style="list-style-type: none"> • Ability to encrypt files/folders on removable media storage devices
	<ul style="list-style-type: none"> • Allows centralized or local management of users and groups

Cryptzone's solution for data at rest protection

Cryptzone's solution for protecting data at rest consists of four separate layers of encryption that work together to provide a complete strategy—the more layers of security that are implemented, the stronger the protection. As with other seasoned forms of information security, such as software protection and identity management, the level of security has a direct and positive correlation to the granularity of the implementation.

Through implementation of Cryptzone's **Data-at-Rest Protection Solution** products, and those of our security partners, protection at all layers can be achieved. Each of the Cryptzone data-at-rest encryption products – Secured eDisk PD, Secured eFile and Secured eCollaboration - offers a robust solution for the protection of sensitive data on laptops, desktops, and removable media devices as well as "network share drives, desktops, and laptops. When used in combination, this family of products can provide a heightened level of security to uniquely address the industry needs of security, usability, and manageability, as well as addressing issues of regional, national, and global compliance.

- **Cryptzone Secured eDisk PD Enterprise Version** encrypts the entire hard drive of laptops, workstations, and removable media to protect against disclosure of information in the case of theft or accidental loss of the hardware device. Pre-boot two-factor authentication with a token or smart card prevents unauthorized users from circumventing the operating system to access sensitive information. Secured eDisk PD provides the choice of local management per workstation or full central management through Microsoft's Active Directory, ensuring that administrators work within a familiar management environment.

- **Cryptzone Secured eFile** is a file and folder encryption that protects sensitive data and creates a secure, centrally managed collaboration platform. Secured eFile enables people to share files and folders securely with individuals and groups inside and outside the organization. The easy-to-use file encryption tool empowers users to secure the information and specify precisely who else in the organization needs access. A central management console allows administrators to deploy security policies across the organization, while built-in technology takes care of managing access rights, user authentication and encryption keys.
- **Cryptzone Secured eCollaboration** is a unique add-on solution for Microsoft SharePoint providing document encryption for documents and access control, creating a secure environment for collaboration. Microsoft SharePoint is a powerful tool for collaboration and content management, but SharePoint does not come pre-equipped with tools for strong encryption or efficient user rights management. Users often store sensitive information in the form of financial data, customer information, project plans, contracts - data that should be protected, on the collaboration platform.

The Cryptzone **Data-at-Rest Protection Solution** products provide a robust security solution from a single vendor—one point of contact for support, customized documentation that simplifies installation and setup, and the elimination of integration challenges. These products are built on mature Cryptzone technologies that have been deployed in small and large enterprises.

Conclusion

The goal of this learning tool was to provide organizations with a better understanding of the importance of protecting that which is the very lifeblood of their business - data. Be it intellectual property, financial information, customer accounts, transactions, or employee or patient information, these assets must not only be protected from compromise, but must also be secured in accordance with current compliance regulations.

By providing information in an easy-to-understand fashion on the issue of data protection, the threats that exist, the regulations that govern, and the solutions that can be implemented, it is our hope that organizations will be better equipped to make the decisions necessary to begin development of a comprehensive security plan.

With Cryptzone's history as a worldwide leader in information security, companies can rest assured that they are investing not only in the highest standard of encryption technologies, but also in a vendor that will be there in the long term to support their security needs as they grow and evolve. Cryptzone is one of the world's largest and most respected security organizations, and one of the few single-source vendors to provide comprehensive and trusted information security products. Cryptzone engineers security tools to be easily administered and transparent to the end user, based on open or common standards whenever possible. Thus, Cryptzone security solutions are designed, from the start, to facilitate - not complicate - business processes.



About Cryptzone

Founded as Secured eMail in 2003, Cryptzone introduced the market's most user friendly and applicable email encryption solution with a single button "Send secured" approach. Following the success of this first simple email encryption application, customers demanded the same ease of use, high performance, scalability and reliability for all sensitive data and not only email. As a result, the company has developed a completely integrated encryption suite coined the Simple Encryption Platform (SEP).

The Cryptzone brand communicates the company's core competence delivered through the centrally managed Simple Encryption Platform (SEP). Cryptzone today offers an encryption solution with modules available to secure email communication as well as securing data on hard drives, USB memory sticks, and granular data in files, & folders network share drives, desktops, laptops, and document on Microsoft SharePoint. SEP enables organizations to integrate all security policies centrally, and deploy new encryption applications in a phased approach both quickly and easily. Cryptzone provides enterprises with a set of applications, middleware, and centralized server-based management to address Data Leak Prevention issues.

For more information, visit www.Cryptzone.com