BOOLE™ server

Vs

Encryption Suites

Introduction

Data at Rest

The phrase "Data at Rest" refers to any type of data, stored in the form of electronic documents (spreadsheets, text documents, etc.) and located on laptops, desktops, mobile devices such as PDAs, smartphones, tablets, or flash drives. These documents are characterized by being in a state of non-transmission and, therefore, are defined as "at rest". Nevertheless, they are exposed to various security risks which one realizes only once the damage is irreparable.

How to protect data

It is widely recognized that the primary causes which expose company data to security risks are increasingly coming from within the company, and are due to a variety of situations: loss or theft of laptops, tablets or smartphones; misappropriation; unauthorized copying or sharing of confidential documents. In this scenario, modern companies have to deal with new security challenges in order to protect their "intellectual property", or simply their own privacy and/or confidential electronic documents. This white paper compares Boole Server with some of the most popular encryption solutions available on the market for the protection and secure exchange of electronic documents.

The software model of encryption suites

The market of products for the encryption of electronic documents or devices (hard disks, flash drives, etc.) nowadays offers many software solutions and tools, even for free, and is able to meet the most various needs of a variety of end users, from single users to small, medium and large enterprises. Each product is characterized by specific *features* according to the context in which it is deployed, and it is more often associated with additional services, such as Cloud solutions or the possibility to centralize and manage security policies from an administrative console.

All the analyzed solutions[1] are characterized by common features in dealing with issues related to encryption and loss/theft of confidential documents:

- ✓ **Encrypting files/folders**: the possibility of encrypting - on laptops, desktops, mobile devices, and tablets - files and/or folders, both in local and in folders shared by users, either in local networks or domains.
- ✓ **Encrypting devices**: the possibility of encrypting entire mass storage devices, such as flash drives, external or internal hard disks. As for internal hard disks, the entire laptop hard disk, for example, is encrypted so that the operating system cannot be started unless password is entered.
- ✓ **Forwarding encrypted e-mails**: the possibility of forwarding encrypted e-mails and attachments to users located both inside and outside the organization.
- ✓ **Security policies**: setting security policies enables organizations to monitor the use of internal resources, in order to limit users' ability to copy or transfer protected information. Through security policies, users can carry out on protected documents only the operations they have been authorized to perform.
- ✓ **Administration tools**: in company environments, both in small and medium organizations, the administrative tools allow to define *ad hoc security policies*, to monitor users' activities or to apply auditing tools.

To implement solutions which allow to encrypt/decrypt messages, files, or plain texts, the *client software* is required: it performs the above listed operations in a transparent manner for the end users. To this end, applications such as PGP by Symantec and many others, apply public/private key encryption algorithms, which are nowadays considered as the safest system[2]. In the most advanced infrastructures, the *client software* has been designed to play the role of **agent** as well, in order to offer additional services for the management of security policies, while enabling communication and updates between the client and the server managing the security solution. When integrated, these components are able to monitor and mitigate the security issues in company environments.

[1] Among the different encryption suites available on the market, this document takes into account encryption software solutions or tools such as PGP, Endpoint Encryption Device Control, Endpoint Encryption Removable Storage Edition by Symantec, Cryptzone, SafeGuard Enterprise and Sophos Data Protection Suite, and Kaspersky.

[2] It has been estimated that (in the case of 1024-bit keys) a network of one million computers would take 10^{10} years to derive a private key from a public key. Therefore, a public key might not be considered as secure only if its real authenticity or belonging are not considered as certain. >> Source: Practical Guide to PGP.

The Boole Server software model

Boole Server is a **Data Centric** software solution ensuring the protection and confidentiality of electronic documents. The server on which it is installed represents *the core of the whole protection system*. It blocks all the channels through which confidential information may be viewed, distributed or manipulated without proper authorizations. In the Boole Server architecture, the server on which the application is installed centralizes and controls all encryption and sharing operations, and implements the fundamental principles for the security of electronic documents:

Absolute Protection: Boole Server offers confidentiality guarantees also in relation to domain administrators or even system administrators. Such profiles are not authorized to access the content of the files users store in Boole Server. Only the file owner and those who are granted with proper authorizations, can access the file content and enable access privileges and sharing modes.

Persistent Encryption: encryption of files, e-mails and attachments through 2048-bit symmetric algorithm. Unlike other encryption algorithms, Boole Server stores the decryption keys centrally, rather than within the files. This is how Boole Server ensures that decryption only occurs through authorized connection to the server possessing the key. Furthermore, Boole Server applies persistent protection on documents even when they are viewed or edited.

Continuous Accessibility: users can access the information protected by Boole Server everywhere and at any time, without running the risk of reducing the security level applied on data. To this end, it is possible to access via Web (Web Client) through SSL communication protocol, the same protocol currently used by the banking industry.

Constant Control: all users and digital documents controlled by Boole Server are constantly monitored. Every user can check, at any time, which operations have been performed on shared documents thanks to an advanced auditing system.

Secure Sharing: Boole Server is revolutionizing document sharing: it does not only allow to select which resources are to be shared, with whom and for how long, but also to assign on one single file differentiated access rights. It is therefore possible to share a document to a user in view-only mode, and in read-only or editing mode to another user. Granularity, selectivity, and possibility to revoke sharing properties in real-time make Boole Server an innovative tool for sharing electronic documents in total security.

The Boole Server architecture is designed to encrypt digital documents, to allow secure and **controlled** sharing, both with working groups and external partners or customers. In order to ensure such a level of security, besides the central server, the Boole Server architecture also implies the use of two other tools: Web Client and Agent.

Web Client: the Web Client is the tool through which users can connect to Boole Server through any Internet browser and benefit of services such as:

- Downloading/Uploading files and folders to/from one's own Boole Server private space; encrypting and/or securing documents.
- Creating and controlling access profiles (this operation is mainly reserved to group administrators).
- Monitoring the activities performed on protected files (Auditing).
- Exchanging messages and attachments in encrypted mode with other Boole Server users.
- Viewing files in protected mode.
- Securely sharing files with other users.

Agent: the Boole Server Agent has been developed to provide additional control and protection on documents while allowing communication between Boole Server and the Client application. The Agent also allows to provide additional functionalities such as:

- Top Secret functionalities to block unauthorized activities, such as "screen capture", and prevent video copying of documents shared in view-only mode.
- Working on files in protected mode.
- Encrypting files in local.
- Creating locally encrypted archives of files.
- Synchronizing a disk in the local company network or domain with centralized resources accessible via Web Client (Remote Drive).
- Encrypting resources in local and generating offline certificates to access encrypted documents even without connection to Boole Server. This operation requires proper authorizations.

Principles of Comparison

The comparison between the different encryption suites and the most innovative Boole Server solution can be summarized in the below check-list which highlights their main differences as well as the features closely related to document encryption, control, and sharing; all features which are not strictly relevant to encryption, such as filters, monitoring or auditing functionalities are not included in this comparison. It is taken for granted that such aspects are already incorporated in all the environments of this comparison, since they refer to security, rather than encryption issues.

Encryption

Description	Encryption suites	Boole Server	Notes
Encrypt **any** electronic document	✓	✓	
Encrypt files stored on **devices**, such as USBs, DVDs or flash drives.	✓	✓	
Create encrypted document **archives**	✓	✓	
Forward encrypted **e-mails and attachments**	✓	✓	
Create **virtual partitions** on HD	✓	✗	Some tools also allow to hide encrypted virtual disks. This is the case of ***TrueCrypt***.
Encrypt files shared in **network shares**.	✓	✓	

Secure document sharing and control

Description	Encryption suites	Boole Server	Notes
Edit in real-time the **sharing** properties of a document already shared.	✗	✓	
Share files with **users external to the company**.	✓	✓	
Work on shared files even in **offline mode**.	✓	✓	Boole Server requires data owners to enable sharing recipients to generate proper offline certificates.
Web access to encrypted files.	✗	✓	
Block "print screen" or "video grabbing" of shared documents.	✗	✓	
Block printing of shared documents.	✗	✓	
Apply **watermark**.	✗	✓	The functionality is available in Boole Server for .pdf documents.
Share encrypted **local archives**.	✓	✓	
View shared electronic documents **in streaming mode** (view-only).	✗	✓	This functionality is currently available in Boole Server only for certain file types[3].
Anti-photo feature.	✗	✓	
Share files in **read-only** mode.	✓	✓	With Cryptzone, sharing files in read-only mode is allowed only if reader role is specified for the recipients of the sharing.
Share documents for a **preset limited time** (minutes, hours, days).	✗	✓	
*Share files in **collaborative mode (limited)***	✗	✓	Files can be shared with other users, who can edit the file content, but **cannot copy it**.

[3] List of file types supported for sharing in streaming mode: **.avi;.bmp;.con;.doc;.docx;.flv;.gif;.tif;.jpeg;.jpg;.mov;.mp3;.mp4;.mp4v;.mpeg;.mpg;.pdf;.png;.pps;.ppsx;.ppt;.pptx;.swf;.tga;.txt;.wav;.wma;.wmv;.xls;.xlsx;.dwg;**

Why to adopt the Boole Server solution

While most of the encryption software solutions have been developed to meet the need of preventing confidential documents to be read unencrypted, Boole Server has approached this issue from a perspective closer to end users' needs. Indeed, Boole Server is an encryption solution which integrates data loss/data leak prevention features, together with built-in functionalities for managing access rights to documents (Information Rights Management). Such integrated features aim at providing precise solutions to customers' problems:

1) Documents are visible by and sharable with specific users or groups only.
2) For a time period set by the document owner (minutes hours, days). After expiry, the document can no longer be used by sharing recipients.
3) How to make documents usable. The document owner can select different sharing modes, including simple sharing, encrypted sharing, or sharing in streaming. They all feature specific additional options such as anti-photo, anti-capture, block of print and/or screen capture, possibility to apply a watermark.
4) Tools for sharing files with users internal and/or external to the company, such as the Web or as attachments to e-mails.
5) Documents can be saved and used in protected mode on iOS mobile devices (iPad and iPhone).

These features make Boole Server™ stand out from other solutions: Boole Server ensures that confidential documents always remain within the company, which thus holds their full control. Moreover, documents remain inaccessible even to system or domain administrators.

Highest usability and company security

Boole Server is the only software solution capable of combining ease of use, security, and control of sensitive data.

For further information about secure file sharing, visit the www.booleserver.com Website or contact Boole Server.