Identifying and Persistently Protecting your Organization's High Value Data

Problem Statement

Organizations share several common security problems when protecting high value data[1].

- Organizations often treat all data the same. The same email system, file servers and laptop hard drives that are used to access high value organizational information are also used to access low risk data. Adding security for one data type means implementing security for all.

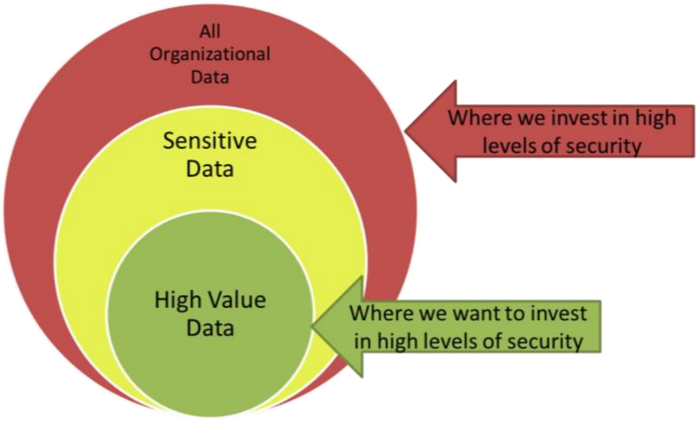
- Attackers are quick to change attack vectors and approach; while organizations are still relying on security developed in the 1990s. Organizations deploy different encryption products for email, VPNs, file encryption, whole disk encryption, etc. Each of these technologies relies on keys for protection. However, each has different sets of keys, and data is left unprotected when passing between the encrypted and secured components. This approach is expensive and protection is not continuous.

- Information flows like water through many networks and across many devices, yet organizations continue to build data silos, focusing on applications and operating systems for protection. Users in organizations are accessing data on laptops, mobile devices, corporate devices, personal devices, moving data to personal email servers, and even personal cloud services that sync to numerous devices outside the organization's control. By leveraging these convenient data sharing technologies, your users are circumventing the IT security controls the organization has invested in.

Despite an ever growing number of headlining data loses, our collective approach to security has changed very little in an era when there have been great advancements to security strategies and technologies. The time to change your organization's approach to data security is now. Old security habits are hard to break, but are costing your organization.

Changing the Approach to Data Security

All data is not the same. You probably already know this, but do not have any means of differentiating the high value data assets from the low value assets on your electronic systems. Here are the steps you can take to stop your organization from relying on outdated IT security approaches:


All Organizational Data
Sensitive Data
High Value Data
Where we invest in high levels of security
Where we want to invest in high levels of security

1) Develop a framework for classifying data inside your organization. Create an organizational Policy Authority to create a common information classification framework for the organization. The first step in focusing security on high value data is being able to identify it.

2) For each data type identify access control rules to be applied to the data. The Policy Authority should determine for each data classification it has defined:

- What types of users should have access to the data – managers only, users in a certain department…
- What type of credential should be required for access – username and password, smart card…

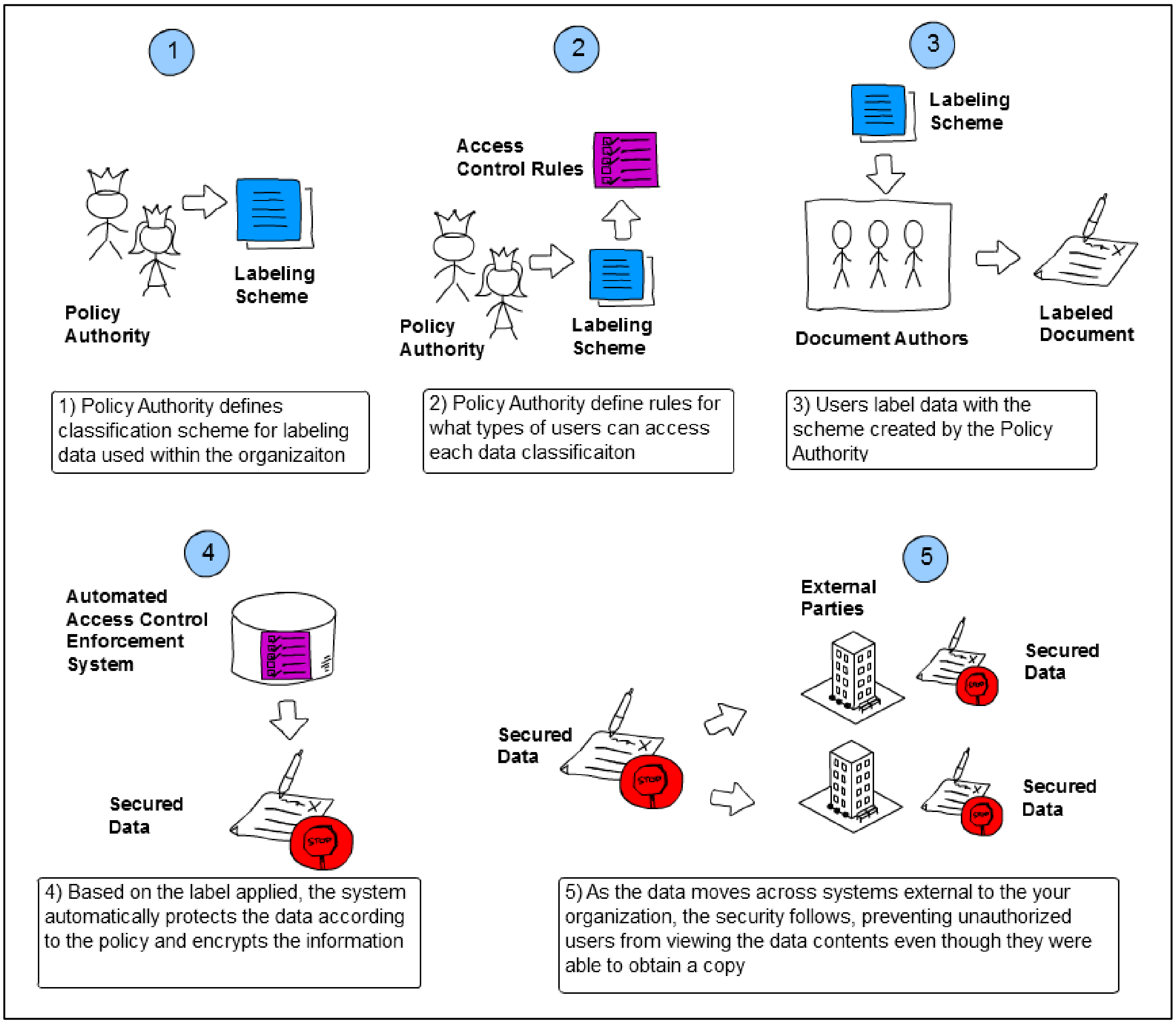
[1] For the purposes of this whitepaper, high value data is defined as information that is critical to the short and long term success of your company, that if compromised can have a distressing impact to your organizations operations.

- Under what circumstances is access allowed – access limited to a period of time, only allowed when users are in a secure building…

3) Have document creators label information using the classification scheme. Labeling information is critical to being able to enforce access control. Labeling includes both visually marking the data for users, but also adding machine readable metadata, that allows computer systems to automatically enforce access controls based on the policy that is applied.

4) Enable an automated access control enforcement service. The access control system will encrypt any data that is labeled as high value, under the defined classification scheme. The protection is enforced on the data itself.

5) Consistent security is enforced as information flows to external networks and organizations. As the labeled and secured document is now emailed, uploaded to file shares, and copied to physical media, the security protections stay with the data. Only users who meet the access control rules are able to open and view the data, regardless of where the data is stored or moved. For example, if a server with high value data is compromised and downloaded by an unauthorized user, the data is still encrypted. When the undesirable party tries to open the data, they cannot do so, even though they were able to obtain a copy.



1) Policy Authority defines classification scheme for labeling data used within the organizaiton

2) Policy Authority define rules for what types of users can access each data classificaiton

3) Users label data with the scheme created by the Policy Authority

4) Based on the label applied, the system automatically protects the data according to the policy and encrypts the information

5) As the data moves across systems external to the your organization, the security follows, preventing unauthorized users from viewing the data contents even though they were able to obtain a copy

Where to Start

Adopting a new approach to securing high value data with persistent access controls can certainly be a challenge. Shifting a security paradigm can be overwhelming to both management and the user base.

- Plan Big, Start Small: When planning how to implement, start with an approach and solution architecture that can scale to support your organization. But when it comes time to deploy, start with a small group of pilot users.
- Seeing is believing: Many of the ideas discussed in this document may seem complex to those unfamiliar with information labeling and automated access control enforcement. However, in practice the new burden to the document authors and readers is minimal. Having a small pilot demonstrator can help bring home concepts that white papers and presentations do not.
- Keep the Information Technology (IT) team closely engaged with the business user: Rarely do IT systems solve problems, if they are not developed in step with the community that will ultimately be using them. IT solutions succeed where there is a high level of engagement between the business users of the infrastructure and the IT team itself. Open honest communication is critical to introducing new solutions to any organization. Where users feel engaged and listened to, there is a far greater openness to adoption, then when a new solution is developed in isolation and presented as a finished product.

For More Information

The technology discussed in this whitepaper is available as commercial-off-the-shelf (COTS) solutions. Electrosoft can help your organization focus and secure high value data, using the practices outlined in this paper.

Please visit www.electrosoft-inc.com for more information on Electrosoft. Or feel free to email us at sskordinski@electrosoft-inc.com.