Understanding the Data Lifecycle: The Key to Effective Data Protection

A Nogacom White Paper

The Data Protection Challenge

Data protection is a key concern for every organization. Companies must ensure that their sensitive information—about customers, personnel, finances, proprietary technology, business strategy, and medical records—doesn't get into the wrong hands. Failure to protect this information can result in lost revenue, lost customers, lost productivity, lost opportunities, and exposure to significant legal liabilities.

Most large organizations, however, have millions of documents, presentations, spreadsheets, emails, and other unstructured data scattered across systems all over the world. Sensitive information may reside anywhere in any of these files. To make matters worse, these files don't just sit still. They are constantly being shared, copied, re-purposed and emailed.

This unstructured data chaos makes it extraordinarily difficult for businesses to effectively protect their sensitive information—because they don't have an accurate, complete picture of what this information is, where it is or what form it is in. As a result, they remain extremely vulnerable to the consequences of both malicious and unintentional data leaks.

There are, of course, many tools available today for preventing data leaks through encryption, access control, and endpoint protection. But these tools can't be used effectively if the organization can't identify their sensitive information or know where it's located.

Organizations also can't create appropriate policies for the access, distribution, storage and management of sensitive data if they don't fully understand how it is actually used on a day-to-day basis throughout its lifecycle. Without this understanding, they will create policies that are either too restrictive—and therefore keeps users from doing their jobs—or not restrictive enough.

In other words, to effectively protect themselves against data leaks, organizations don't just need data protection tools. They need a rational, fact-based data lifecycle protection process.

Only through such a process can organizations answer the key questions necessary for effective data protection, including:

- Which files contain sensitive information?
- Where are these files located?
- Who is accessing these files?
- Who is making copies and creating new versions of these files?
- To whom are these files, copies and versions being sent?
- Why is the above activity taking place?

Companies that can get complete, accurate and up-to-date answers to these questions can successfully protect themselves against data leaks. Those that can't will remain exposed—no matter how sophisticated their data protection tools may be.

NogaLogic for Data Lifecycle Protection

Nogacom's leading-edge NogaLogic information governance solution provides organizations with granular visibility into their unstructured data assets. This information gives companies the necessary insight to understand their information risks, then define and implement effective data governance policies and business best practices - based on their users' real business needs and their actual data assets. This insight also helps companies to optimally configure their data protection tools so they can effectively identify and protect their sensitive business information throughout its lifecycle.

NogaLogic helps organizations assess their exposure to information risk:

- Accurately identify all sensitive business information—including all copies and versions
- Understand how documents containing sensitive information are being used across their organizations
- Create effective policies that map to business needs, based on the real business value of the information
- Mitigate business risk without impeding the legitimate use of information
- Reduce the cost and effort of information security operations
- Facilitate effective communication and cooperation between IT, security and business users to achieve common goals

A Proven Methodology for Data Lifecycle Protection

NogaLogic's rich functionality supports a structured methodology for data lifecycle protection:

Identify and Assess the Data

The first and most important step is to identify sensitive information and to assess how it is currently being used. NogaLogic does this by:

- **Automatically discovering and classifying all documents requiring protection**. NogaLogic's powerful data classification engine automatically identifies and classifies all documents based on their business context and value to the organization. Through this process NogaLogic can specifically identify and isolate certain documents which, because of the nature of their content, are considered sensitive by the business, such as proprietary business information, financial documents, or customer information. NogaLogic can also automatically identify documents containing multiple pieces of information, which together make the document sensitive, such the combination of a person's contact information together with a certain medical condition that he or she has , as well as documents containing sensitive regular expressions, such as credit card numbers, ID numbers, banks account numbers etc
- **Automatically identifying copies and versions of documents.** This allows data and security managers to see if someone in R&D is creating copies of proprietary product plans using unexpected filenames—and to then find out why.
- **Automatically tracking the distribution of documents via email.** This allows data and security managers to quickly see if, for example, a user bypassed the organization's secure VPN and instead emailed documents to a personal Gmail account in direct violation of corporate data security policies.
- **Automatically mapping where sensitive data is being stored.** Data and security managers can use this information to discover inappropriate file storage anomalies—such as salespeople saving customer contracts to their personal directories, when they are supposed to save them to SharePoint.
- **Automatically detecting who has access to sensitive business files.** This allows data managers to understand how data is being accessed—and if, for example, users still have access to sensitive files even though their job responsibilities have changed.

Define Data Protection Policies

Once an organization has granular visibility into the current state of its unstructured data assets, it can then intelligently define appropriate policies for protecting its sensitive information without creating excessive restrictions that undermine the ability of users to get full business value out of the data assets they need to do their jobs.

Certain policies, such as policies that move sensitive business documents to a secure data repository, can be defined and implemented through NogaLogic itself—using its native automated content-based document classification and/or any other user-defined parameters. Other policies should be defined by the company's data protection tools.

NogaLogic can also be used to apply meaningful security classifications—confidential, top secret, public etc — to documents for data protection purposes. For example, NogaLogic can identify all documents containing information about a new secret product and automatically classify them as "confidential." All policies pertaining to "confidential" documents will then be automatically applied to those documents and can be then used by company's data protection tools.

Enforce

Once effective policies have been defined, they can now be applied to the data using the company's data security and protection tools, such as access control, DLP, encryption etc.

Monitor, Measure, Adjust, Re-assess

With NogaLogic, organizations can continuously monitor their information risk and measure the effectiveness of their data security policies over time to discover instances where sensitive information has not been adequately protected, and/or instances where policies have impeded legitimate business use. They can then respond to these issues by fine-tuning policies, changing business practices, educating users, or by making a conscious decision to accept certain known risks in order to gain certain known business benefits.

NogaLogic also helps organizations to respond to changes in their businesses—such as corporate re-structuring, M&A activity, and/or new regulatory mandates. In addition, NogaLogic can help organizations more readily discover possible misuses of sensitive information and, if necessary, perform required security forensics.

Visibility Throughout the Data Lifecycle

Organizations can't effectively protect their sensitive information—no matter how much they invest in data protection and other security technologies—if they don't know exactly where it is. They can't avoid over-restrictive policies if they don't know exactly how their data is actually being used today. And they won't be able to implement essential protections if doing so requires too much time and effort and negatively impacts legitimate business use.

NogaLogic helps companies address all of these issues by providing them with the critical visibility needed into their unstructured data throughout its entire lifecycle. By enabling organizations to identify and better understand how their sensitive information is being stored, accessed and distributed every day, NogaLogic uniquely empowers them to mitigate risk, reduce IT costs, and ensure that users have continuous access to the knowledge they need to do their jobs.