NEXTLABS®

White Paper

Managing Information Risk for Microsoft SharePoint

Protecting Data, Streamlining Compliance, and Gaining Visibility

"If not stored, protected, harnessed and metered effectively, information is wasted, weakens in value, or can pose many risks. Information governance has become a business imperative, and company leaders' ability to apply equal rigor to managing all components of information across the business information supply chain will affect business performance, partners and prospects."

Toby Bell, Debra Logan, and Ted Friedman
Analysts, Gartner, Inc.

INTRODUCTION

Enabling Collaboration with Microsoft SharePoint

Ease of use, simple administration, and powerful collaboration capabilities have driven rapid adoption of Microsoft SharePoint. Companies find that once they make SharePoint available, the number of sites grows quickly. Many companies report having more SharePoint sites than employees. The explosive nature of SharePoint can catch data owners and information managers off guard, especially when it comes to ensuring that sensitive information is protected once it is shared.

SharePoint was designed to operate as an "adhocracy,"1empowering the end user by enabling collaboration, innovation, and results. However, when using SharePoint to manage sensitive intellectual property and automate regulated business processes, there are common challenges to solve:

- Protecting intellectual property (IP) managed in SharePoint
- Sharing sensitive information externally with customers and partners
- Controlling access across SharePoint sites to support company policy or regulatory requirements
- Enforcing data segregation in compliance with data residency requirements dictated by export or data privacy laws
- Auditing and monitoring thousands of independent sites for compliance

Balancing Collaboration and Governance

Given these challenges, companies often struggle with controlling the use of SharePoint while driving collaboration. When governance is applied with a heavy hand, companies sacrifice the innovation, creativity, and efficiency that SharePoint's ad-hoc model promotes. Striking the right balance between collaboration and governance or is the key.

INFORMATION GOVERNANCE OBJECTIVES

Information Governance is the set of policies and procedures that ensure that corporate information is protected, used effectively, and handled in compliance with company or regulatory requirements. The most common Information Governance objectives for Microsoft SharePoint deployments include:

1. Proper Classification of Data

Companies are increasingly challenged with how to manage their data. As more data is collected and shared, it has become increasingly difficult to ensure data is available to the right person at the right time. To meet the needs for access to data from anywhere, anytime, and any device, companies must classify their data. Access policies can then be defined based on the different classifications of data.

2. Enforced Segregation of Data

Companies often need to control where data can be uploaded or downloaded based on the classification of the data. Data privacy or export regulations may mandate certain sensitive data to be located in-country. Thus, the ability to enforce data segregation can ensure compliance with data residency requirements and prevent toxic data spills.

3. Policy-Driven Authorization for Data (Entitlements)

Access to data shared on SharePoint is often governed by permissions. Managing permissions is onerous, particularly as the number of groups and volume of data increases. Additionally, companies are increasingly wanting to manage access to data based on the sensitivity of the data, and other attributes such as project membership, skills certification, location of access, and nationality of the user, which cannot be easily managed through existing group-based policies. Companies need authorization policies that can control access at the data level based on these different attributes or claims to ensure compliance and confidentiality.

4. Protection for Intellectual Property

More and more company intellectual property (IP) is being managed in SharePoint, including design documents, sales tools, technical documentation, pricing, marketing plans, budgets, company strategy, and even customer data. While SharePoint provides some permissions and information policies, the use of these tools is at the discretion of end users or individual site administrators. Studies show that users do not consistently protect sensitive data once the user has accessed or downloaded it from the server. To protect IP, companies need to:

- Prevent leakage of IP beyond people that “Need to Know”
- Limit access to external partners, customers, or contractors who collaborate via SharePoint based on fine grained decision attributes such as nationality, security clearance, roles and project membership
- Control access and usage of documents that have been downloaded from SharePoint sites

5. Reduced Cost of SharePoint Audits

As the amount of data managed in SharePoint increases, so does the requirement to audit it for Sarbanes-Oxley, export control, customer contractual obligations or other compliance requirements. Even if the company has a policy of not using SharePoint for regulated business processes, there are no effective controls to prevent users from using it to share these controlled documents. To reduce the cost of audits, companies look to:

- Centralize administration of access rights to streamline audit reporting
- Audit and monitor end-user activity, providing effective controls and reporting evidence of incidents

MANAGING INFORMATION RISK ON MICROSOFT SHAREPOINT

A Comprehensive Solution

The NextLabs Information Risk Management solution for Microsoft SharePoint extends SharePoint Services to help companies achieve their Information Governance objectives. Key solution capabilities include:

1. Identify, Classify, and Mark Data

Automatically discovers and classifies data in SharePoint, including sites, pages, lists, libraries, items, and documents. Classification can be used to drive access and storage controls, as well as enable persistent protection outside of SharePoint.

2. Segregate Data by Policy

Policy-driven data segregation controls ensures data is uploaded or downloaded based on data classification. Data segregation enhances compliance with regulatory mandates, such as data privacy and export control laws, by automatically segregating data and ensuring appropriate data residency.

3. Entitlement Management

Centrally-managed, policy-based access control across SharePoint sites and servers enhances the native security model of SharePoint by enabling attribute-based authorization to SharePoint data. Attribute Based Access Control (ABAC) enables powerful rules that authorize users based on multiple factors, for example, classification of the file, user attributes, claims, and even dynamic factors such as device or network location.

An ABAC rule may state, "Allow only Engineers on Project Destiny, located in US or UK, to access parts classified as Project Destiny." When a user attempts to access a document classified as Project Destiny, no matter where the file is stored in SharePoint, this rule is validated in real-time with no perceptible latency.

4. Integrated Enterprise Digital Rights Management (EDRM)

The NextLabs solution provides end-to-end protection of intellectual property using Integrated EDRM. EDRM automatically applies rights protection to documents in SharePoint. Once protected, document-level access and usage controls will persist with the file, no matter where it is downloaded or distributed.

5. Centralized Audit and Reporting

Automated audit of user activity and pre-built reports provide insight into policy violations, user activity, and access rights, and reduce the effort associated with internal or external audit for compliance.

6. Powerful Policy Management

The NextLabs solution enables centralized management of information control policies that govern end-to-end data access and usage. These policies are automatically enforced across all SharePoint sites and on other enterprise applications such as Windows File Server, Windows desktops, and Outlook.

Case Study 1: Intellectual Property Protection for Microsoft SharePoint

An engineer downloads a highly confidential CAD drawing to her desktop for review. She inadvertently copies the drawing to a public file server, exposing the IP to everyone in the company. Another employee takes the file from the public share and sends it to a friend who works for a competitor.

With NextLabs, the downloaded document maintains its access control so even users with access to the public share cannot access the file. Policy can also be used to ensure the file remains protected even if it is emailed outside the enterprise so an unauthorized user cannot open it or share it again.

Case Study 2: Microsoft SharePoint Audit

A financial accountant creates a SharePoint site to manage financial spreadsheets used for period end reporting. Access to financial spreadsheets is based on multiple attributes such as job role, country and sensitivity of the financial data. Across time, team members change roles, in some cases creating violations to Segregation of Duty requirements. Auditors demand evidence of changes to access permissions.

With NextLabs, a policy can be used to control access to the financial data based on role, country and con-tent. Access is dynamically authorized and no longer requires a site administrator to make manual changes to permissions of individual documents. All access to financial spreadsheets are also automatically tracked and reported to auditors.

Case Study 3: Microsoft SharePoint Entitlements

A SharePoint Administrator in IT provisions a departmental site for the Engineering organization and as-signs a Site Administrator. Months later, there are 150 individual sub-sites, each with their own administra-tor and permission settings. When an employee transfers out of the engineering department, there is no simple way to revoke access to engineering data.

With NextLabs, a company policy limiting access to Engineering employees can be created at the top-level site regardless of what individual site administrators do. Access can be automatically taken away when an employee changes roles or departments. In addition, any change to access permissions performed by site administrators are logged for audit purposes.

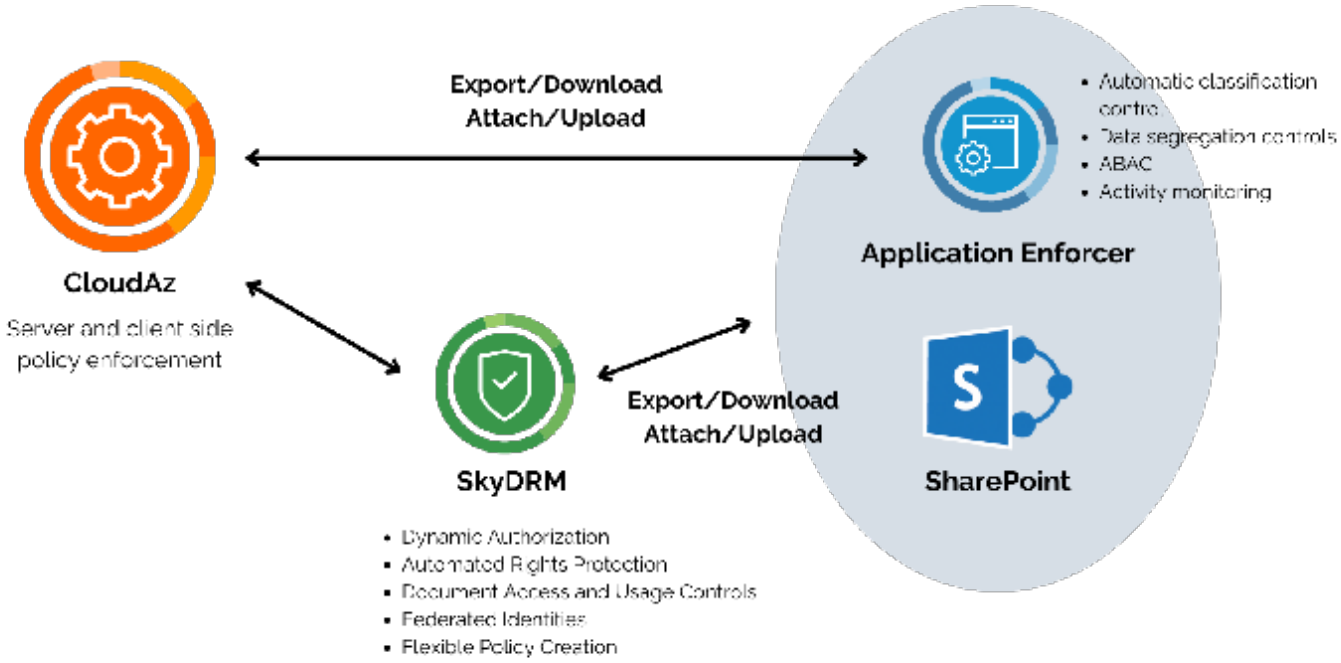
SOLUTION COMPONENTS

1. Server and Client Side Policy Enforcement

The Information Risk Management solution for Microsoft SharePoint includes the NextLabs Application Enforcer and SkyDRM for Microsoft SharePoint.

Application Enforcer for Microsoft SharePoint integrates natively with SharePoint Services to enforce and automate fine-grained authorization policy across all SharePoint objects, including site collections, sites and sub-sites, lists, document libraries, list items, documents, announcements, calendars, tasks, and more.

The NextLabs SkyDRM enables secure collaboration for sensitive documents flowing through internal and external business processes by automating access and usage controls across enterprise applications, cloud applications, and endpoints. It protects sensitive documents stored in the cloud, providing features such as controlling access rights to documents in real-time, automated rights protection and federated identities.



2. Out of the Box Reporting

A pre-built set of reports is available to provide Data Owners or Information Managers visibility and audit for SharePoint. Audit is simplified with policy reports that summarize policy violations and access rights.

Report Server

Report Server provides a central repository for enterprise-wide auditing. All activities logged by the Policy Enforcement software are collected in a central data warehouse to provide a single comprehensive source for investigation and analysis.

Reporter

The web-based reporting application enables analysts to generate charts and reports showing SharePoint access rights, access attempts, authorization decisions, end-user activity, and trend analysis. It is able to create and share policy and activity reports, including summary, trend, and detailed event analysis. This reduces the cost of responding to auditors, legal inquiry, or incident investigation.

Microsoft SharePoint Information Governance Reporting

3. Standards Based Policy Management

Policy Studio

Policy Studio is a graphical application for Microsoft SharePoint policy management across sites and servers. It is an easy-to-use, drag-and-drop policy management tool for editing, deploying, and managing policies. Policy Studio speeds up policy development and increases productivity.

Central Policy Server

The XACML-based Policy Server is an open, standards-based policy repository and management server that centralizes SharePoint governance policy and system management at the policy administration point (PAP). It is built with a scalable distributed architecture that easily integrates into existing IT infrastructure, including Active Directory and SharePoint for discovery.

Distributed Policy Controller

The Policy Controller is a distributed, cross-platform policy decision point (PDP) that provides real-time policy evaluation on servers and endpoints. The distributed architecture of the Policy Controller and the optimized deployment technology makes the NextLabs Information Risk Management solution for SharePoint the most scalable entitlement management system available, with support for hundreds of thousands of enforcement points. The solution is very cost effective for use in large enterprises and is complementary with existing ITAR, EAR, and similar regulatory compliance solutions.

SOLUTION BENEFITS

With NextLabs Information Risk Management solutions, companies can achieve balance between ad-hoc collaboration and governance on Microsoft SharePoint. Some of the benefits provided by the solution include:

- Centralized entitlement management that ensures consistent authorization to SharePoint data aligned with company and regulatory policy
- Secure collaboration, both internally and externally
- Protection of critical data, so SharePoint can be leveraged for even the most sensitive projects
- Automated implementation of information controls that simplify data access governance, eliminate mistakes, and reduce cost
- Comprehensive visibility into events and data for audit, oversight, and troubleshooting

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit http://www. nextlabs.com