Information Rights Management and Document Control

Solution Brief

Improve visibility and collaboration while ensuring confidentiality of planning and manufacturing data

OVERVIEW

Ease of use, simple administration, and powerful collaboration capabilities have driven rapid adoption of Microsoft SharePoint. Companies find that once they make Microsoft SharePoint available, the number of sites grows quickly. However, the explosive nature of Microsoft SharePoint can catch data owners and information managers off guard, especially when it comes to ensuring that sensitive information is protected and that the use of Microsoft SharePoint supports company goals.

Given these challenges, one can under-stand why some would want to clamp down on Microsoft SharePoint use by setting up bureaucratic hurdles to its adoption. However, when governance is applied with a heavy hand companies sacrifice the innovation, creativity, and efficiency that Microsoft SharePoint's ad-hoc model promotes. Striking the right balance between ad-hoc collaboration and governance is the key.

SOLUTION HIGHLIGHTS

- Proactive Protection of Intellectual Property. Stop data loss in real-time, online or off-line, by controlling document access and usage.
- Information Barriers Support. Controlling document access and usage is essential in ensuring the integrity of barriers or "Chinese Walls" that define safe and secure communication and collaboration areas and prevent in-formation export.
- Rapid Policy Update and Deployment. Easy to use policy authoring; networkfriendly policy deployment.
- Persistent Proactive Protection. Same policy is enforced on servers, desktop, applications, mobile devices.
- Simple Data Security with Interactive Remediation. Automate remediation to deliver real-time policy educa-tion, data classification, data cleansing and encryption, and much more.
- Audit and Incident Investigation. Detailed endpoint activity logs to reconstruct sequences of events across systems and users to investigate incidents and compliance hurdles.

THE SOLUTION

The Information Governance for Microsoft Office SharePoint solution meets this challenge. It comprises five key applications that enable corporate policy objectives for protecting information, while promoting open, ad hoc collaboration. These include:

- Intellectual Property (IP) Protection for Microsoft SharePoint
- Entitlement Management for Microsoft SharePoint
- Microsoft SharePoint Extranet Security
- Audit for Microsoft SharePoint
- Information Lifecycle Policy for Microsoft SharePoint

COMPONENTS

The Microsoft SharePoint Information Governance Solution consists of the following components:

Policy Adapters

Policy Adapter for Microsoft Office SharePoint Server - The Policy Adapter for Microsoft Office SharePoint Server is policy enforcement software that integrates with Microsoft SharePoint Services or Microsoft Office SharePoint Server (MOSS) to monitor access, export, upload, and download activities across Microsoft SharePoint site collections, sites, lists, document libraries, documents, and items. It extends Microsoft SharePoint's access control system to provide centrally managed, fine grained, identity-based authorization to Microsoft SharePoint applications and data.

Application Enforcer for Microsoft SharePoint - The Application Enforcer for Microsoft SharePoint is policy enforcement software that runs on desktop and laptop machines to enforce fine-grained entitlements to data after it leaves the Microsoft SharePoint Server.

Control Center Policy Server Platform

The Information Governance for Microsoft Office SharePoint solution runs on the NextLabs Control Center, a XACML based policy server platform that provides central management of policies and procedures. The Control Center provides:

- Policy Server - Policy administration point (PAP) where policy and procedures are centrally managed.
- Policy Studio - Graphical policy development and management toolset.
- Enrollment Manager - Extensible integration manager for enterprise policy information points (PIP). Provides pre-built connectors to common attribute sources such as Active Directory and LDAP directories.
- Report Server - Centralized activity journal where activity and audit information is collected, analyzed, and reported on for automated compliance auditing.

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 Policy Controller provides critical services to policy enforcement points (PEP) for policy evaluation, security, and management. These services are available to application developers using the Policy Adapter SDK. Our Policy Controller is designed for high throughput across a wide range of deployment scenarios, including offline devices, on multiple platforms.

Dashboards and Reports

- Role-based dashboards for IT security, compliance officers, and data owners summarizing data use and policy violations.
- Activity analytics provide reports filtered by user, department, data resource, and policy, with summary and trend analysis.
- Detailed activity reports provide granular details of user activity for forensics and incident investigation.

SOLUTION DEPLOYMENT: HOW TO GET STARTED TODAY

NextLabs provides services to implement the Solution in your particular environment by using expert product knowledge and a services best practices methodology. NextLabs can also assist clients with identifying their controlled data, as well as defining information control policies.

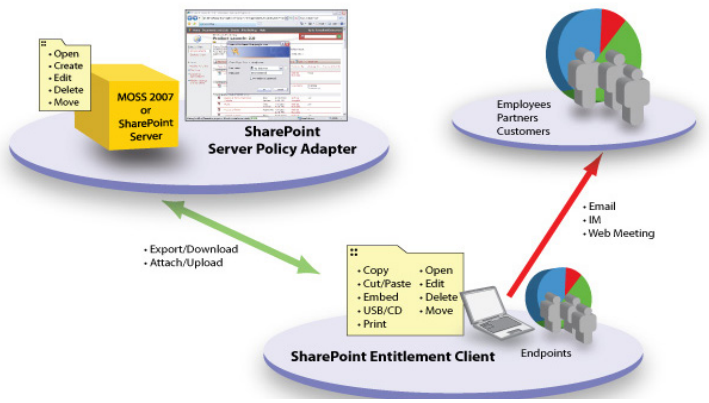
Step 1: Requirements Gathering - NextLabs works with you to understand your infrastructure, and security and policy requirements.

Step 2: Risk Assessment - We help you to discover and identify your current risks to help prioritize Solution requirements.

Step 3: Policy Configuration - Policies are designed and electronically codi fied using Enterprise DLP™, along with any custom Policy Assistant automation.

Step 4: Install Policy Enforcers - Policy Enforcers are deployed across applications and systems, if applicable to requirements.

Step 5: Knowledge Transfer - Finally, NextLabs helps train your team to maintain the Solution.



NEXTLABS® | Zero Trust Data-Centric Security

ABOUT NEXTLABS

NextLabs®, Inc. provides zero trust data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based zero trust 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, AWS, Accenture, Deloitte, Infosys, and IBM. For more information on NextLabs, please visit: **http://www.nextlabs.com**.