



Application Enforcer for SharePoint

Enforce ABAC & Externalize Authorization



OVERVIEW

Microsoft SharePoint provides a popular platform for sharing business-critical data. Teams enjoy easy, ad-hoc collaboration with rapid SharePoint site creation, user provisioning, and a discretionary access control model. Yet, the boon to business collaboration also amplifies the risk that sensitive, regulated, and highly valuable data will be leaked or mishandled.

THE SOLUTION

NextLabs Application Enforcer for SharePoint is a SharePoint extension that provides a more granular level of information governance to safeguard your most sensitive information. NextLabs automates information controls on SharePoint data to enable secure collaboration:

- Automatic classification controls that identify and classify data uploaded to SharePoint.
- Data segregation controls that limit where sensitive data can be uploaded to avoid toxic data spills.
- Attribute-based access controls (ABAC) that make authorization decisions based on attributes of users, devices, data classification, IP address, etc.
- Automatic application of document controls that persistently protect data even after it leaves SharePoint.
- Activity monitoring provides visibility to where new sensitive data resides, what controls are in place, and who is accessing the data.

THE RESULTS

The benefits of more advanced information governance in SharePoint include:

- **Secure Collaboration**, both internally and externally, with customers, partners, and other third parties.
- **Protection of Critical Data** so SharePoint can be leveraged for even the most sensitive projects.
- **Automated Information Controls** that simplify data access governance, eliminate mistakes, and reduce cost.
- **Comprehensive Visibility** into events and data for audit, oversight, and troubleshooting.

KEY FEATURES

POWERFUL POLICY MANAGEMENT

Application Enforcer for Sharepoint is built on the NextLabs CloudAz platform, which deploys powerful policies to govern end-to-end data access and usage from enterprise applications to any endpoints.

AUTOMATICALLY IDENTIFY, CLASSIFY, AND MARK DATA

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

EXTEND SHAREPOINT WITH ATTRIBUTE-BASED ACCESS CONTROL

Application Enforcer for SharePoint extends SharePoint container-based permissions with Attribute-Based Access Control (ABAC). 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 Project Destiny engineers located in the US or UK to access data 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.

INTEGRATED ENTERPRISE DIGITAL RIGHTS MANAGEMENT (EDRM)

Application Enforcer for SharePoint offers unsurpassed data protection using Integrated Enterprise Digital Rights Management (EDRM). Integrated EDRM automatically applies rights protection to documents in SharePoint. Once protected, document-level access and usage controls will persist with the file, regardless of where it is downloaded or distributed.

CENTRALIZED AUDIT AND REPORTING

Policy compliance and end user activity are collected in a central Activity Journal for reporting by NextLabs Reporter, a graphical analysis, charting, and reporting application

TECHNICAL SPECIFICATIONS

Component	Support
Microsoft SharePoint versions	Microsoft SharePoint Server 2016 Microsoft SharePoint Server 2019
Authentication Methods	<ul style="list-style-type: none">Windows Integrated AuthenticationClaims-Based AuthenticationForms-Based Authentication (FBA)Web Single Sign-on (SSO)Active Directory Federation Services (ADFS)
Access Protocols and Clients	<ul style="list-style-type: none">Browser (HTTP protocol, webdev, REST API, CSOM)WebDavWeb FoldersMicrosoft FrontPage Server ExtensionsMicrosoft Office, including Office web and mobile applicationsWeb Services (CSOM clients, REST API)
Operating System	<ul style="list-style-type: none">Windows Server 2016, Enterprise EditionWindows Server 2019, Enterprise Edition
NextLabs Product Compatibility	<ul style="list-style-type: none">CloudAzCEPC/Java PC

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>.