NEXTLABS®

Microsoft Outlook Enforcer

Enforce ABAC & Externalize Authorization

OVERVIEW

Communication applications, such as email and instant messaging, are a common channel for data loss. Businesses driven by regulations and customer requirements must separate communications completely between groups of employees, partners, and customers to prevent conflicts of interest. Furthermore, businesses need to collaborate between groups, but fear the consequences of leaking confidential data by sending it to the incorrect recipients.

THE SOLUTION

NextLabs Microsoft Outlook Enforcer is policy enforcement software that integrates with Microsoft Outlook to monitor and control email communications and document distribution. It works in the background without needing user attention and interacts only when a policy requires the user to follow proper information handling procedures.

- Granular Identity-Based and Document Attachment Controls to ensure the right people get the right information.
- Real-time, Preventive Enforcement to warn and advise users and/or block unauthorized actions.
- Automated Remediation so end users can classify, encrypt, remove hidden data, and perform operations themselves in an interactive wizard; no need to involve IT or create manual workflows.
- Activity Monitors provide visibility to into all events for compliance reporting and auditing.

THE RESULTS

- **Implement Precise Information Barriers -** Avoid conflicts of interest and maintain compliance when sending emails and documents between groups of employees, partners, and customers.
- **Prevent Miscommunications -** Enforce identity-based policy to prevent unauthorized or unintended emails based on sender and recipient relationship.
- **Simplify Security -** Automated real-time policy education, recipient validation, data classification, data cleansing, encryption, and more.
- **Secure Collaboration -** Rights Managed files are secure no matter where they are, even when downloaded outside of communications.
- **Centralized Visibility -** Track email and file distribution from sender to recipient.

Help end-users perform remediation tasks with interactive wizards, simplifying email security and improving policy enforcement.

Task	Detail
Hidden Data Removal	Cleanse metadata by removing comments, revisions, & other hidden data from attachments
Recipient Verification	Verify recipients to prevent miscommunications with inappropriate recipients
Misdirected Document Distribution	Prevent sending documents to the wrong client or customer
Document Classification	Tag document with user selected class or automatically classify based on content
Attachment Encryption	Apply encryption on-demand based on who is sending what to whom
Append Notice	Append disclaimer or confidential notice in subject and message body
Email Header Tag	Add custom tags to email headers for server-side processing
Policy Communicator	Deliver policy education with immediate feedback about information handling procedures
Strip Attachment	Based on the classification, content, size, type and recipients, automatically strip the attachment and replace it with a URL for the document. The documents can be uploaded to FTP site, SharePoint, File Server, Box and Dropbox
Automated Rights Protection	Automatically apply policy-based rights management depending on business requirements and classification of data

KEY FEATURES

PROACTIVE COMMUNICATION CONTROL

Monitor and control activity at the endpoint to block miscommunications in real-time, thereby reducing audit and incident investigations.

- **Alert:** Alert user when policies apply and educating about relevant policies
- **Warn:** Warn user and let user decide to proceed with an action
- **Block:** Stop user from performing an action and inform user about policy

IDENTITY-BASED COMMUNICATIONS CONTROL

Control communications between senders and recipients based on both party's user name, email address, group membership, assigned roles, or any user attribute defined in enterprise directory, such as Active Directory, to prevent unauthorized communications between them.

FINE-GRAINED ATTACHMENT CONTROL

Prevent sending the wrong attachments by selecting the right data to protect with precise, fact-based data identification:

- **Location:** Local, remote shares, or mapped drives and folders
- **Classification:** Public, confidential, restricted, etc.
- **Content:** Search keywords and patterns
- **Attribute:** Document tag to identify customer or use any custom property

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.

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.