SkyDRM for Exchange

Protect Data at Rest, Shared File, and Payload

OVERVIEW

Exchange is a powerful email and calendaring server developed by Microsoft. It is designed to provide business-class email, calendar, and collaboration solutions. Exchange provides a robust email platform that supports large volumes of email traffic, ensuring reliable and efficient communication within and outside of the organization. Customers often need to share business documents as attachments in email with external partners to enhance productivity, improve innovation and increase cost-effectiveness.

Even though sharing business documents with external partners provides these business advantages, it can also introduce potential security risks, including the following:

- **Data Breaches**: If an external partner's security measures are inadequate, sensitive business information can be exposed to unauthorized parties.
- **Intellectual Property Theft**: Proprietary designs can be stolen or misused by partners or third parties.
- **Compliance Violations**: Sharing sensitive information without proper safeguards can lead to violations of data protection regulations, resulting in legal and financial penalties.
- **Supply Chain Attacks**: Cyber attackers can target external partners to gain access to design documents, exploiting vulnerabilities in their systems.

THE SOLUTION

To mitigate these risks, it is crucial to implement strong measures such as:

- **Data Encryption**: To protect data both in transit when it is shared and at rest.
- **Access and Usage Controls**: Implement the principle of least privileged access, limiting access to sensitive documents to only users who need them.
- **Regular Audits**: Conduct regular security audits of partners to ensure compliance with security standards.

NextLabs' SkyDRM is Enterprise Digital Rights Management (E-DRM) designed to protect data in use, in transit, at rest and when shared across extended enterprises with audit capabilities. With SkyDRM, any file type can be protected and accessed from any device to ensure secure collaboration with access and usage controls. SkyDRM integrates seamlessly with Exchange through a Rights Management Extension (RMX) to enforce security policies on the Exchange Server to secure email and meeting invite data sharing across different platforms and applications like Outlook, mobile devices, and Outlook Web App (OWA).

KEY FEATURES

KEY FEATURES	
Classifying and Rights Protection	Classify and protect email attachments based on classifications derived from the following sources: • User-defined classifications • Keywords in the email subject, body, or attachments • Custom properties in the email attachments • Email X-header information • MPIP (Microsoft Purview Information Protection) label of email message or attachments
Remove Protection	emove SkyDRM protection on email attachments based on email sender's permission on the protected documents
Centralized Visibility	Centralized monitoring and reporting on data use for full visibility

KEY COMPONENTS

KEY COMPONENTS	
SkyDRM Rights Management Server (RMS)	SkyDRM Rights Management Server provides end-to-end protection of sensitive data with authorization, rights protection, rights enforcement, and document activity monitoring
SkyDRM RMX for Exchange	SkyDRM RMX for Exchange enforces security policies on the Exchange Server to secure email and meeting invite data sharing across different platforms and applications like Outlook, mobile devices, and Outlook Web App (OWA)

BENEFITS

BENEFITS	
Secure Information Sharing	Enable product data to be securely shared between design partners, suppliers, foreign employees, joint ventures, and customers worldwide by providing policy-driven protection and an end-to-end audit trail
Improved Compliance	Improve compliance and governance programs by automating information controls for sensitive product data with a comprehensive audit trail
Complete Data Protection	Protect sensitive data by controlling access and usage as data moves across organizations and enterprises
Rapid Deployment and Adoption	Deep integration and zero-code client installation allows for rapid deployment among the extended partner networks

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.