NEXTLABS®

White Paper

A New Approach to Digital Rights Management: Enterprise DRM

Enterprise DRM (E-DRM) is often referred to as Information Rights Management (IRM) and addresses the data protection needs of a different environment: the enterprise. Enterprise Digital Rights Management (E-DRM) systems protect enterprise information from unauthorized access, use and distribution by applying rules to the information distributed in electronic documents.

Unlike consumer DRM where rights are embedded initially before distribution to protect media as a whole, E-DRM policies selectively prevent document recipients from specific use activities like copying, printing, forwarding, cut & paste, and expiration. Policies can be updated or revoked even if the document has been distributed outside the enterprise. E-DRM is frequently used to reduce exposure to information risks and prevent data loss when communicating and collaborating with partners. E-DRM protects information against theft, misuse, or inadvertent disclosure, and mitigates the business, legal, and regulatory risks of collaboration and information exchanges with partners and customers. With logging capabilities to support auditing, E-DRM systems are also used to demonstrate compliance and due care.

Enterprises rely on electronic documents not just as the means to share and disseminate information but also to collaborate. Enterprises create and consume content created by its workforce and share it with business units across the enterprise and with trust partners and customers. It is critical to limit distribution and use of certain classes of documents to certain groups or users inside and outside the enterprise.

One of the primary advantages of electronic documents is their ease of movement, but businesses need to control document content and ensure that the document does not fall into the wrong hands, or the content is not used improperly. Enterprises are looking for a DRM solution that can combat this data leakage by going a step beyond encryption by adding controls to the use of the content of a document (not just protecting the file itself), and without losing the fluid communication characteristics of electronic documents – for example: allow viewing of a document but limit editing and partial duplication of the content by certain users or group of users.

Most DRM products adopt a tethered client-server model that is based on a license server with a DRM client framework. The licensing server handles the cryptographic key, which is required to access the protected content. The client that attempts to access protected content has to connect back to this licensing server to access this key. Content access is authenticated via the license server. This means that the authentication mechanism is tied to the license server and not the content. As such, the content is tied to the license server.

For sharing information inside the company, enterprises often integrate DRM products with PKI or a Directory Service infrastructure. This can be costly and time-consuming. However, there has not been a viable and efficient approach to manage policy and implement controls for sharing with or distributing to users who are not on the corporate network and PKI system. While outside the company firewall, and without reliable network connectivity to a license server, recipients may require access to protected documents. The accessibility to a license server, as required by tethered DRM systems, severely restricts the use of DRM. Some progress has been made by tethered systems to resolve this issue (namely caching of licenses), but this does not improve transparency overall, since caching requires that users know that they will be without a connection and attention to cache management is required by both the end user and system administrator.

A New Approach to DRM Is Needed

While DRM has matured over more than a decade, it has yet to reach a tipping point of widespread adoption in enterprise markets. The technology falls short in its deployability, usability, flexibility, and interoperability to meet enterprise requirements.

However, there has been an increasing demand for a better DRM solution to deal with the increasingly more complex need to mitigate information risk and protect data throughout enterprises. As a result, the marketplace is seeking a new breed of DRM product.

Traditional DRM systems protect documents by encrypting the document and providing control of access by embedding the policy with the document. However, the reliance on encryption results in an increase in complexity and expense associated with key provisioning, recovery, authentication, and effective management of the encryption keys for each user. Additionally, DRM systems adopt a tethered architecture and the requirement to log onto a license server and remain online severely restricts the use of DRM. Tethered DRM systems require an end user to have network connectivity to access a protected document (unless the document has date restrictions in which case connectivity may again be required to check the time against an internet time server).

DRM products often employ proprietary languages or schemes to specify information access and usage policies, but enterprises demand open standards for interoperability, integration, and multi-sourcing to prevent lock-in to a particular product or vendor.

Most DRM products defined policy based on pre-defined users or user groups but lack identity-awareness in the ability to inspect content, and leverage knowledge of user context in evaluating policy and making policy decisions. This lack of identity-awareness results in the inability to define policy based on user attributes, organization structure, and employee identity. These systems overlook role, user, group, device, content, application, location, and other elements in policy decisions, resulting in high number of policy and manual process to update policy to keep up with the user and organizational changes. Collectively, these factors often complicate enterprise deployment and significantly increase the Total Cost of Ownership (TCO). This high degree of maintenance is very error-prone, and results in under-enforcement by leaving gaps in data security policy. Additionally, the imprecise applications of policies can also impose constraints to business processes and frustrate end users.

DRM solutions can address low level security but lack an identity-driven approach. Current DRM products cannot fully address high value business collaboration scenarios across multiple communication and collaboration channels. These scenarios include preventing external data loss, protecting intellectual property, preventing conflicts of interest, enforcing information barriers, and many more information protection requirements necessary to support regulatory compliance.

Many DRM systems employ specific platform or content format-centric designs that protect native data or applications well. But large enterprises deploy a heterogeneous information technology environment so DRM systems must interoperate with a variety of platforms, systems, document formats, and furthermore, with existing enterprise infrastructure like directory services, key business applications and legacy applications as well.

Usability and transparency to the end users is critical to prevent interruptions to business processes and achieve high levels of user acceptance. Transparency of operation affords several benefits in terms of usability, including ease of-use for the end user in applying protection and ease-of-access for the document recipient. Any DRM product that needs minimal or no end user intervention in applying protection is more likely to be used than a product that requires extra steps to apply the protection.

End user adoption has always represented a significant risk to successful DRM deployment because DRM systems do not interact with end users nor apply workflow to assist end users. DRM systems today do not support transparency of operations and burden users with the task to assess and set the usage rights consistently for documents before communication and distribution. Untrained or undisciplined content creators often forget to use DRM or apply policies in a haphazard fashion to avoid disruption in their business processes. Successful DRM deployment depends upon end user acceptance of changes in business processes and backed by rigorous and frequent user training. Consequently, a large-scale deployment of DRM often requires changes and interruptions to the ongoing business processes of both users and IT during deployment and use.

Despite the benefits that current DRM systems can provide; it is still too complex and costly to deploy for the enterprise. The new requirements coupled with the shortcomings of the traditional IRM products have limited applicability and wide-spread adoption of IRM in the enterprise. Therefore, a new approach to DRM is needed.

THE NEW APPROACH TO DRM

To fully extract the benefits of DRM, a simpler, more manageable, user friendlier and more enterprise ready approach is needed. This paper looks at a new approach to DRM and key issues with traditional DRM that needs to be addressed. It examines what DRM needs to provide to be effective in satisfying the needs of today’s enterprises.

An effective DRM solution should provide the core functionality of traditional DRM but at the same time, meet the following requirements:

1. Works across all file types and applications
2. Flexible and Dynamic Identity-Based Policy
3. Content Awareness
4. Interoperability with Enterprise Identity and Access Management (IAM)
5. Support for both Internal and External Collaboration
6. Easy Enterprise Deployment and Management
7. Open standards architecture to support untethered operation Improved End User Productivity
8. Improved End User Productivity
9. Compatibility with the Information Lifecycle Management
10. Dynamic Authorization to control access rights based on Zero Trust Principle

1. Works across All File Formats and Applications

Enterprise IT environments handle data in many formats and employ a variety of business applications. Yet many DRM solutions are designed to protect data from specific applications in specific file formats. This ignores the fact that some of the most critical data in the enterprise exists in unsupported file formats such as source code files, CAD drawings, or text files. Suite providers may provide DRM solutions that work well with native content authored with their own tools but provide a varying or confusingly inconsistent level of user experience when the end user works with content in formats created by other applications.

In comparison, the new approach to DRM is format and application agnostic, providing the same, consistent, high level of user experience across data formats and applications. This approach prevents the proliferation of different DRM systems for different data formats and application types. It vastly reduces the cost of policy development by ensuring that one policy can be applied similarly across applications and data as necessary.

2. Flexible and Dynamic Identity-Based Policies

Many DRM systems base policy on fixed users or explicitly defined user groups. This assumes that the person applying protections to a document actually knows who may need to access this information in the future – perhaps even years from now. Most companies are much more dynamic than this - employees come and go and frequently change roles or assignments. With traditional DRM, each of these changes requires explicit, manual policy changes.

The new approach to DRM is flexible, dynamic and identity-based, making authorization decisions based on the role or attributes of a user by leveraging identity data that is managed in enterprise identity management systems or directories. Authorization is not based on who you are (e.g. John Doe), rather it is based on what you are (e.g. Manager of Project X). In this model, enforcement automatically adapts as the users move in and out or an organization or change roles.

3. Content Awarenes

DRM solutions have no understanding of what the content is of the documents they protect. Rather, they assume that the end user will manually apply policy to each and every document if they know that it contains sensitive information. For companies trying to protect specific classes of information, such as Personally Identifiable Information, Personal Health Information, Financial Data, or Intellectual Property this assumption is not realistic.

The new approach to DRM will automatically apply protections to data based on its content. This approach has several significant benefits. Obviously, it protects the right information all of the time. In addition, is simplifies policy management by reducing the number of policies to be proportional with the number of classes of data, typically tens or hundreds, rather than the number of documents, typically millions or billions. Also, this approach greatly enhances end user productivity, but removing the burden of having to remember which data needs DRM and needing to manually apply it.

4. Interoperability with Enterprise Identity and Access Management (IAM)

DRM systems are typically access control policy islands. The policy created in them has no direct relationship with the access control rules set up on the servers with which the data is managed or originates, requiring companies to manage the same business rules in multiple systems. Part of the issue is that today’s DRM solutions are based on proprietary policy languages and lack integration with existing Enterprise IAM infrastructure. In the long term, this lack of interoperability and compatibility results in vendor lock-in, or silos of policies or data, and risks from technology obsolescence. This problem is further aggravated when business policies are codified in a static proprietary policy language that may not be exportable to other systems.

In contrast, the new approach to DRM employs open, standards-based policy language. The leading language is the Extensible Access Control Mark-up Language (XACML), a product of the OASIS standards body. Undergoing its third major release and enhancement, this XML based language is designed to support information access control policies and has received major industry support as an open standard adopted by all of the leading enterprise technology providers including IBM, Oracle, Cisco, SAP, and others. Businesses that employ DRM systems built upon XACML benefit by protecting their investments in their policy libraries, simplify integration with enterprise IAM and other third-party applications, future-proofing their investment in policy development.

5. Supports Internal and External Collaboration

Today's business processes often cross company boundaries, as sensitive information is shared with partners and customers in distributed supply chains or collaborative workflows. Unfortunately, current DRM solutions don't support both internal and external collaboration. They can be used to share information with specific external users, but don't work well when that user needs to edit, analyze, or manipulate the data or share the information with other co-workers.

In contrast, a new approach would allow information to not only be shared with external users, but external organizations or teams and allow the information to be used and manipulated by not only the specific user, but also by other users within the external organization.

6. Easy Enterprise Deployment and Management

DRM systems have proven to be difficult to deploy and expensive to manage. There are two fundamental reasons for this. First, traditional DRM design requires that each document be known and encrypted. In today's organizations this amounts to billions of files scattered across the organization. Managing licenses (encryption-keys) for each and every document makes the cost of managing the system proportional to the amount of data. Many companies find that they need to create, manage, and maintain hundreds of thousands of policies and millions of licenses. And once all of these files are encrypted, you are stuck – there is no getting out without potentially losing a lot of important data.

The new approach to DRM is designed to easily scale with the amount of data. The number of policies is proportional to the number of business use cases – not the amount of data. The management of encryption keys or licenses is minimized making it easy to apply, manage, migrate, and recover protected data.

7. Open Standards Architecture to Support Untethered Operation

As mentioned earlier, most DRM products adopt a tethered client-server model that is based on a license server with a DRM client framework. The client that attempts to access protected content has to connect back to this licensing server to access this key. Content access is authenticated via the license server.

Because the authentication mechanism is tied to the license server and not the content, information availability is compromised when network connectivity is unavailable or unreliable. In a global collaborative supply chain environment, many business partners capable of delivering product at low cost also reside in nations where the communications infrastructure may be lacking.

If network connectivity is unavailable or unreliable, access to content will also be unreliable, impacting productive collaboration and business agility. In addition, the mobile workforce of today's enterprise requires that information is constantly available and accessible, but employees, partners and contractors may be working offline or outside the company firewall, with limited network connectivity.

In contrast, the new DRM approach is designed from the ground-up, using open standards-based implementation to operate efficiently in a mobile enterprise environment of globally distributed workers and partners, even under offline usage or conditions of uncertain or unreliable network connectivity. DRM clients should be capable of fast and precise policy evaluation; even while offline, outside the firewall, or without network connectivity.

8. Improved End User Productivity

End user adoption has always represented a significant risk to successful DRM deployment. In user centric DRM systems, users take the role of specifying rights, and so user training becomes critical. Successful DRM deployment depends upon end user acceptance of changes in business processes which now require the unending discipline and motivation to assess and set the usage rights consistently for documents themselves before communications and distribution.

Consequently, a large-scale deployment of DRM often requires changes and interruptions to the ongoing business processes of both users and IT during deployment and use. Untrained or undisciplined content creators may simply forget or refuse to use DRM, or worse, use DRM but apply policies in a haphazard fashion, simply to avoid disruption in their business processes.

The problems associated with the user centric model for specifying policies are worsened by current DRM systems' dependence on network access to validate encryption key with the license server. This requirement interrupts the transparent nature of the protection process and makes it harder to use for the end users. Although caching can be used as a 'fix' for this loss of transparency, the caching mechanism still requires both connectivity to the server, at some point, and the foreknowledge to cache security policy licenses with expiration dates, etc.

If the protection process can be fully automated and made invisible to the end user, and eliminate end user intervention, then application of security policies can be managed transparently and enforced by the enterprise through the IRM system.

In the new approach, a DRM system has the ability to interact and collect feedback from end users and provides integrated workflows that can automate information handling procedures like the application of encryption or DRM protection upon content. Other information handling may be automated as well as part of an overall data protection strategy including automated hidden data removal, proper information destruction, misdirected email prevention, etc. With helpful automation that assists the user in their business process objectives, the new approach to DRM ensures the satisfaction of the end user with the welcomed adoption of this helpful tool.

9. Compatibility with the Information Lifecycle Management

A key risk with the use of DRM is in enterprise recordkeeping. Critical in the content lifecycle, an enterprise retains a substantial volume of archival data, content, and email as records. Recordkeeping has significant operational, compliance and legal implications for a business, and especially a government agency.

However, archiving DRM encrypted content as records risks data availability. Access to these records may be constrained through inappropriate or outdated policies, hardware and software dependencies, or simple loss of decryption keys due to employee turnover or physical catastrophe, effectively results in the loss of records.

An organization may not be able to maintain DRM encrypted information, especially evidence received, as evidence in a business transaction or for adequate record-keeping. DRM protected information may not be portable or migrated to future platforms (e.g. disabling printing, email forwarding disabling), may not be rendered or converted in other formats. The protection may result in the illegal disposal of official records if a document expires ahead of retention schedules. Inaccessible documents may run afoul of any Freedom of Information Acts or prevent access by investigative authorities such as the law enforcement or the courts.

The new DRM approach controls the access and usage of information throughout its entire lifecycle. It manages and enforces enterprise-wide information policy, and selectively calls for encryption services when situations warrant. When ready for archive, automation capabilities under the new DRM approach can ensure content is decrypted or alert a records manager of any issues prior to archival of the record. This ensures compatibility with the corporate information lifecycle.

The new approach to DRM should also work with document classification and data cataloguing tools. By integrating DRM with data catalog and document classification tool, enterprises can create a comprehensive security framework that spans the entire lifecycle of its data. This helps enforce data governance policies, meet compliance requirements, and protect sensitive information from unauthorized access or distribution throughout its journey within the organization. DRM working with data cataloguing and classification tools can ensure access rights and security policies are consistently applied to classified data throughout its lifecycle.

Equally important, is the ability for DRM to automatically classify and label un-classified documents based on content, context, and sensitivity. These labels serve as the foundation for enforcing precise access control policies, ensuring that only authorized individuals can access, modify, or share classified documents. Moreover, through integrated labelling tools, organizations can seamlessly apply data classification labels, such as “Confidential,” “Internal Use Only,” or “Public,” to their digital assets. This approach empowers organizations to enforce access policies according to the assigned labels, such as restricting access to “Confidential” documents to users with the appropriate permissions.

10. Dynamic Authorization to Control Access Rights Based on Zero Trust Principle

Dynamic authorization is pivotal in the context of DRM, offering efficient access control that departs from static models. It evaluates real-time contextual factors like user location, device type, access time, and behavior to make informed access decisions, ensuring better alignment with evolving security needs. This approach allows for adaptive access policies, automatically adjusting access rights, and fine-grained control, enabling precise rules for users, devices, and data resources. Applying dynamic authorization with DRM results in more scalable and sustainable solution due to a significantly lower number of encryption keys and policies as well as change requests required to protect a high volume of data.

Combining DRM with dynamic authorization is in alignment with the principles outlined in the Zero Trust Architecture by NIST. DRM with the use of dynamic authorization determines based on the identity of the recipient(s) and the characteristics of the data accessed, what permission and user action are granted to control user from specific use activities like viewing, modifying, printing, forwarding, making a copy, extracting content, and expiration.

The combination allows for dynamic access control as users, devices, and/or applications are verified in real-time at each access attempt-following the “never trust, always verify” principle. Additionally, dynamic authorization and EDRM can protect data at rest and in transit while enabling “least privilege access,” granting users, devices, and applications the least amount of access required to perform their jobs effectively. In doing so, DRM and dynamic authorization play into the “assume breach” principle, limiting lateral access and protecting data across the network, system, application, and file repository.

NextLabs’ Zero Trust Data-Centric Security and the new Approach to DRM

NextLabs Zero Trust Data Security Suite is a comprehensive suite of access enforcement and data protection applications powered by a zero-trust policy platform. It enables organizations to protect critical data at the source, in use, on the move and at rest.

NextLabs Enterprise Digital Rights Management (E-DRM) solution - SkyDRM, delivers on the 10 key requirements for the next generation of the E-DRM. The solution provides persistent control of access and usage of digital information stored in files regardless of where it exists. It can safeguard and monitor any document regardless of file type ranging from business document to intellectual property and product design, wherever it lives or travels – across devices, data centers, apps, cloud services, and on-premises.

NextLabs SkyDRM advances the role of dynamic authorization within the E-DRM landscape, offering a comprehensive Information Rights Management (IRM) application that allows companies to control and audit information access and use, even after sensitive data has left the server. Using SkyDRM, companies can enforce cross company E-DRM policies to limit access to data (including expiration), clipboard operations (cut, copy, and paste), printing, and automatically apply digital watermarks within and outside of the corporate network.

Additionally, SkyDRM supports multi-domain attribute-based policies for flexible access and seamless integration of workflows without disruptions to provide end-to-end protection across partner networks, accelerate supply chain collaboration without risking IP leakage and ensure compliance through centrally tracking of data access and usage activities across the extended enterprise.

SkyDRM's approach to DRM removes the fundamental limitations that have hindered the deployment of DRM technologies. It works for any file type, any application, and provides a unique policy enforcement model that makes the solutions relevant for both internal and external collaboration on a single system that is easy to deploy and manage. The table on the next page describes how SkyDRM makes DRM usable for even the most demanding and complex enterprise.

Comparison of NextLabs SkyDRM with Traditional DRM

Requirement	NextLabs SkyDRM	Traditional Digital Rights Management	Benefits with NextLabs
Works Across All File Types and Applications	Enforcement is application and file type agnosti	Protection limited to specific known vendor, specific applications and formats. No support for text files, source code, and CAD drawings	Addresses all sensitive data with a single solution
Flexible, Dynamic Identity-Based Policy	Dynamic policy based on existing identity data including user roles, assignments, and attributes. Policy associated with what you are, not who you are for dynamic environments	Fixed policy based only on users and groups. Requires explicit policy changes anytime someone's role or assignments change	Reduces policy management costs by 10X Improves end user productivity by making data available to the right people at the right time Addresses governance and compliance requirements directly
Content Aware	Able to control access and use of documents based on their content (e.g. Personally Identifiable Information, Source Code, and Financial Data)	No understanding of document content. Controls need to be manually applied to each and every document	Reduces policy management costs by 10X Improved productivity as protection is applied automatically to the right data
Interoperates with Enterprise IAM	Based on the XACML open standard with integration to leading identity and access management systems	Proprietary policy systems with integration to a single vendor technology stack (e.g. Microsoft). No integration to any other access management systems	Interoperability Future-proof investments Lower management costs by eliminating policy silos

Requirement	NextLabs SkyDRM	Traditional Digital Rights Management	Benefits with NextLabs
Support Internal and External Collaboration	Policy and control can be applied to internal employees as well as external partners and customers, without requiring infrastructure federation	Requires customers or partners to deploy tightly integrated IRM infrastructure, which is typically not possible	Protects data even in distributed, collaborative business processes
Easy to Deploy and Manage	Solutions can be deployed with a small number of dynamic policies and zero encryption key management	Requires management of document keys for each document under control. Policies need to be written for every document and every user or group	Reduces policy management costs by 10X. Eliminates risk of data "shredding" caused by complex encryption key management
Open standards architecture supporting untethered operation	Supports enterprise mobile workforce enabling information availability, by protecting content whether in online or offline mode during communication and collaboration Enhances collaboration over extensive global supply chain by supporting and usage inside and outside of the company firewall or over less reliable network infrastructure Fast and precise policy evaluation; event while offline, outside the firewall, or without network connectivity	Tethered client-server (license server and IRM client) framework. Requires network connectivity to authenticate clients and provide content keys Use of IRM restricted to tethered clients, ease-of-use impacted Dependency to encryption key, therefore subject to complexity and cost of encryption and key management Unreliable access to content due to requirement for network connectivity	Reduces cost and complexity as encryption, key or cache management is not required Authorized access to protected content is maintained whether online, offline, outside the company firewall for productive collaboration Provides broader applicability and lower barrier for enterprise-wide adoption Allows anyone, in any location, to share the secured information and provide more flexible architecture that allows a more natural and fluid system to evolve, evoking the way that humans naturally work
Improved End User Productivity	Protections automatically applied based on policy Policy Assistants automate data security procedures to educate and assist end users with document protection tasks Capability to interact and collect feedback from end users	Requires end users to remember and manually apply protections	High end-user adoption Improved productivity Greater compliance Ease of use and high user acceptance. Transparent access to content

Requirement	NextLabs SkyDRM	Traditional Digital Rights Management	Benefits with NextLabs
Compatible with Information Lifecycle Management	Automated assistants for selective application of encryption works with data retention and backup Work with data cataloguing and classification tools to ensure consistent application of security policies throughout the data's lifecycle	Encryption is incompatible with enterprise archiving and backup DRM protected information may not be portable or migrated to future platforms	Compliance with information lifecycle and records management Ensure only authorized individuals can access, modify, or share classified documents
Dynamic Authorization to Control Access Rights based on Zero Trust Principle	Allows for dynamic access control where users, devices, and/or applications are verified in real-time at each access attempt, following the "never trust, always verify" principle	Lack the capability to determine access rights, continuously monitor, and assess the trustworthiness of users, devices, and applications during an active session	Simplify policy management and reduce # of policy and encryption key significantly Limit attack surface, making it difficult for attackers to move laterally within the network or access sensitive information Reduce administrative burden of managing complex access control lists and permissions Real-time risk assessment to respond quickly to potential threats

LEARN MORE

Learn more about the new approach to Digital Rights Management in the enterprise and NextLabs SkyDRM:

- SkyDRM Brochure: https://www.nextlabs.com/wp-content/uploads/SkyDRM-Brochure.pdf
- Information Rights Management and Document Control Solution Brief: https://www.nextlabs.com/wp-content/uploads/SB-IRM-and-Document-Control.pdf

Our team of enterprise information security experts at NextLabs will help you evaluate your needs, clarify key objectives, and recommend the fastest path towards meeting your solution requirements.

Request a preliminary risk assessment of your enterprise information with our team at: https://www.nextlabs.com/talk-to-an-expert/

GLOSSARY

Access Control or Access Rights Policy

Access control or Access Rights policies define the rules and restrictions for accessing and using electronic documents.

Consumer DRM

Consumer DRM is used to protect media by embedding rights before distribution to protect the content as a whole.

Data Classification

Data classification involves categorizing data based on its sensitivity and importance to apply appropriate security measures.

Data Encryption

Data encryption is the process of converting data into a coded form to prevent unauthorized access. It involves using algorithms and keys to transform data into an unreadable format, ensuring its confidentiality and integrity.

Data Leakage Prevention

Data Leakage Prevention (DLP) is a strategy for preventing sensitive data from being shared or exposed to unauthorized individuals.

Digital Rights Management (DRM)

DRM is a technology that protects digital content from unauthorized access, copying, and distribution.

Document Recipients

Document recipients are individuals who receive electronic documents with specific use restrictions, preventing actions like copying or forwarding.

Dynamic Access Control

Dynamic access control adapts to real-time conditions and user attributes to determine access rights.

Dynamic Authorization

Dynamic authorization allows for real-time control of access rights based on the Zero Trust Principle.

Enterprise DRM (E-DRM)

Enterprise Digital Rights Management (E-DRM) systems protect enterprise information from unauthorized access, use, and distribution.

Information Governance

Information governance involves managing and protecting data throughout its lifecycle, including retention and disposal.

Information Lifecycle Management

DRM solutions should be compatible with information lifecycle management to ensure data security and accessibility.

Information Security

Information security encompasses strategies and technologies to protect data from various threats and risks.

Policy Enforcement

Policy enforcement ensures that security policies are consistently applied to protect electronic documents.

Policy Updates

E-DRM policies can be updated or revoked even after document distribution, enhancing security and control.

Zero Trust Architecture

The Zero Trust Architecture philosophy emphasizes verifying access to enterprise resources continuously, aligning with dynamic authorization.

Zero Trust Security

Zero trust security refers to an evolving set of network security paradigms that focus on protecting resources rather than network segments. It is a response to the rise of remote users and cloud-based assets that are not located within an enterprise-owned network boundary.

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.