NEXTLABS

SOLUTION BRIEF

Pharmaceuticals and Life Sciences

Protect highly sensitive intellectual property and automate GxP compliance through the use of automated, real-time policies.

SOLUTION BENEFITS

- **Protect intellectual property**
  Prevent disclosure to unauthorized users and apply access and usage controls on documents
- **Increase business agility**
  Automate change management processes to expedite responses to changes in business requirements
- **Secure global collaboration**
  Enable the secure sharing of data between employees, partners, and suppliers via digital rights management
- **Reduce security and compliance costs**
  Eliminate the need to implement and maintain costly customizations to meet security and compliance requirements
- **Streamline IT management**
  Reduce the time, resources, and cost of IT management by utilizing more automation and contextual controls

OVERVIEW

Bringing new drugs to market is time-consuming, expensive, and fraught with risk, not least because of the significant regulatory constraints imposed on pharmaceutical and life sciences companies.

For instance, "GxP" was created by the US Food and Drug Administration (FDA) to provide guidelines and regulations for ensuring that pharma products are "safe, meet their intended use, and adhere to quality processes during manufacturing, control, storage, and distribution."

GxP guidelines are driven by three key elements: traceability, accountability, and data integrity. Currently, pharma companies rely on manual controls and processes for data gathering, monitoring, and reporting, making it very difficult to remain in compliance with applicable regulations. Additionally, manual approaches do not scale well, especially given the exponential growth in data and the need to secure sensitive intellectual property (IP).

The financial payoff can be tremendous if a drug successfully makes it to market. This is why introducing automated controls to meet security and compliance requirements is so crucial. Besides protecting IP, pharma companies also stand to benefit in other ways:

- Increasing employee productivity and the business' overall agility
- Enabling secure collaboration across globally distributed stakeholders
- Streamlining IT to support corporate initiatives

THE SOLUTION

NextLabs Entitlement Management and Digital Rights Management solutions provide end-to-end data protection for leading business-critical applications such as SAP, Siemens, Microsoft, and Slack, among others. Through its patented dynamic authorization platform, organizations can leverage contextual controls and centralized policy management to improve their security and compliance posture for several enterprise applications.

The Entitlement Management solutions prevent unauthorized access to sensitive data in critical business applications through fine-grained access controls, allowing customers to protect data and address compliance requirements at the same time.

The Digital Rights Management solutions enable secure collaboration between partners, vendors, customers, and multi-tier supply chains. They enable employees and external partners to share critical information, encouraging collaboration, boosting workplace productivity, and increasing business agility.

Both sets of solutions employ automation to manage and protect data, including automated data discovery and classification, real-time monitoring and policy enforcement for access control, and automated logging and reporting. Ultimately, security and compliance management are made more efficient.

CONTROLS THAT UNDERSTAND THE CONTEXT OF INFORMATION USE

Protecting IP is difficult when devices, data, and users (including customers, partners, and suppliers) are globally distributed. But, applying and enforcing policies based on context, such as identity, data type, activity type, and location, gives organizations the granularity and flexibility needed to respond quickly to ever-changing business requirements.

NextLabs' solutions include:

- **Contextual Access Controls**
  Solutions that control access to data based on context (e.g., group, department, employee status, citizenship, data type, device type, IP address, etc.) are known as attribute-based access controls (ABAC) and offer more granularity and flexibility than role-based access controls. The net effect is that organizations utilizing ABAC can make smarter, more accurate decisions based on real-time information.

  Example: Ensuring that only authorized users can access the IP of certain drugs. NextLabs' solutions can block access to those users that haven't gone through the required certification and/or training, avoiding costly non-compliance penalties and decreasing monitoring and detection costs.

- **Persistent Data Protection**
  NextLabs enables the protection and monitoring of sensitive data, such as IP and R&D findings, wherever it resides or goes – across devices, apps, cloud services, or on-premises.

  Confidentiality is preserved even as IP is shared in joint-development efforts with partners. Safe and approved channels are enforced to maintain data integrity while the data is in transit – and while being used at the destination site.

  Example: Pharma Company A has a joint R&D agreement with Pharma Company B. They have to send sensitive R&D findings to each other. However, not every employee at Pharma Company A should have access to R&D material from Pharma Company B. Granular access and usage rights to specific documents need to be applied, such as who can view, print, and edit certain files.

- **Activity Monitoring**
  Protection includes activity monitoring and controls for conflicts of interest to ensure IP from one project does not "leak" into competing and/or unrelated projects.

  Example: Pharma Company has several projects going on at any one time. However, Research Associates should not be able to access every single project. They should only be able to access projects to which they are assigned. NextLabs can monitor access attempts by project and log activities accordingly.

- **Automation of Change Controls and Compliance Approvals**
  Data handling processes and procedures are applied, including the initiation of proper workflow processes for gaining project approvals and complying with change management procedures.

  Example: Pharma Company wishes to maintain an audit log of all access activities for the company's projects. NextLabs can monitor access attempts by project and log activities accordingly. Additionally, auto-generated compliance reports can be set up.

AUDITING & REPORTING

Comprehensive auditing helps ensure project lifecycle and program confidentiality and compliance with standards and contractual agreements. Forensic analysis capabilities help discover and identify abnormalities during the lifecycle.

Auditing and reporting capabilities allow questions such as the following to be answered:

- What are the primary repositories that contain IP?
- When is a user allowed to copy and print sensitive data?
- What were the attempted email destinations besides designated client or project domains?
- Where and how is information leaked at endpoints (copy, upload, USB, etc.)?
- When were R&D documents accessed and used, including sender and recipient information, timestamps, attachments, etc., during their lifecycle?

SOLUTION DEPLOYMENT: HOW TO GET STARTED TODAY

NextLabs implements its solutions by leveraging deep product knowledge and a best practices methodology for services. NextLabs assists clients with identifying their sensitive data as well as creating the appropriate information control policies.

Step 1: Requirements Gathering

NextLabs works with customers to get a thorough understanding of their infrastructure, security posture, and policy requirements.

Step 2: Risk Assessment

NextLabs helps customers discover and identify current risks to help prioritize solution requirements.

Step 3: Policy Configuration

Policies are designed and electronically codified.

Step 4: Deployment of Controls

Policy enforcers are deployed across business applications and systems to protect data.

Step 5: Knowledge Transfer

NextLabs offers training so that organizations can maintain the solution after it has been deployed.

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.

NEXTLABS