Solution Brief

Intellectual Property Protection

Prevent intellectual property misuse and improper disclosure with a single policy set to manage controls, inside and outside the enterprise, for enabling safe and compliant project team collaboration

SOLUTION HIGHLIGHTS

Identify gaps in protection Investigate IP access and handling, uncover misuse, and demonstrate policy compliance

Preserve IP confidentiality Prevent disclosure to unauthorized users and locations

Avoid conflicts of interest Maintain competitive advantage and client reputation

Educate users and automate procedures. Avoid indiscretion when IP is accessed and used during PLM

Extend protection to outside of the network Extend data mobility, supply chain & remote user protection

OVERVIEW

Intellectual property such as development research, CAD/CAM designs, source code, and strategic business plans are a company's most important assets. When IP is leaked, companies suffer competitive disadvantage, lost sales momentum, and damaged reputation.

But today's basic access controls do little to prevent data loss after authorized user access is granted. Problems include:

- Files are uploaded to FTP sites without proper approvals
- Inability to comprehensively monitor IP access and handling
- Information is uploaded to unapproved websites/portals
- IP is copied to unapproved removable media (e.g., USB devices)
- IP is being sent over email and IM to improper recipients

It is unrealistic to expect users to always manually follow procedures to protect sensitive data. Management overhead, a lack of coordination, and human error all increase the risks of losing sensitive data.

THE SOLUTION

Companies can now protect IP by ensuring safe and appropriate data access, use, and disclosure during PLM. The Solution applies business policies across repositories where IP is stored, and endpoints and applications where used. The Solution enforces controls across heterogeneous applications and systems, such as PDM, document respositories, and CAD/CAM applications, to protect IP throughout its entire lifecycle. Solution support includes Microsoft Windows and Office, Linux, and PLM products such as NX 4, SolidWorks, AutoCAD, Pro/E Wildfire, Allegro, and more.

Companies can now unify access entitlements and data handling policy. The solution educates users about policies and procedures, and automates protection when teams collaborate, while remaining transparent to normal business.

CONTROLS THAT UNDERSTAND CONTEXT OF INFORMATION USE

Preventing IP misuse is difficult when devices, data, and users are mobile, or if users, customers, partners, and the supply chain are spread across multiple locations. Policies are enforced by evaluating context, such as identity, data type and activities, and business conditions, in real-time, to apply precise controls.

The Solution includes:

Internal Collaboration Barriers

Protection includes conflict of interest activity monitoring and controls to ensure IP from one project does not leak into designs of competing products.

Change Control Automation and Approval Compliance

Automated data handling processes and procedures are applied, including initiating proper workflow processes for gaining project approvals and complying with change management procedures.

Confidentiality across Extended Enterprise

Protection is maintained when IP is shared outside the project, including preventing improper disclosure across the extended supply chain. Safe and approved channels are enforced to maintain data integrity in transit and protection is applied while IP is used at the destination.

Endpoint Data Loss Prevention

IP check-out/download must be to approved locations, and only exported to removable media, printed, copied, uploaded, and so forth, if authorized. Policy Assistants help to automate safe access and handling, while users are educated to use data properly.

Communication and Distribution Data Loss Prevention

IP distribution and communications are limited to only secure, approved applications and channels to avoid leakage.

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 to be answered, such as:

- What are the primary repositories that contain IP?
- What are the user exception cases for copying and printing?
- Where is IP attempted to be e-mailed outside of designated client or project domains?
- How often are files uploaded or FTP'd to locations outside of the project domains?
- Where and how is information leaked at endpoints (USB, copying, uploaded, etc.)?
- When were design documents accessed and used, including tracing the lineage of documents during their lifecycle?

SOLUTION DEPLOYMENT: HOW TO GET STARTED TODAY

NextLabs® implements the Solution by using expert product knowledge and a services best practices methodology. NextLabs will assist clients with identifying their controlled documents, as well as defining information control policies.

Step 1: Requirements Gathering

NextLabs works with you to understand your infrastructure, and security and policy requirements.

Step 2: Risk Assessment

We help you to discover and identify current risks to help prioritize solution requirements with clear visibility into your environment.

Step 3: Policy Configuration

Policies are designed and electronically codified, along with any custom Policy Assistant automation.

Step 4: Install Controls

Policy Enforcers are deployed across PLM, and business applications and systems, to protect data.

Step 5: Knowledge Transfer

Finally, NextLabs helps train your team to maintain the Solution.

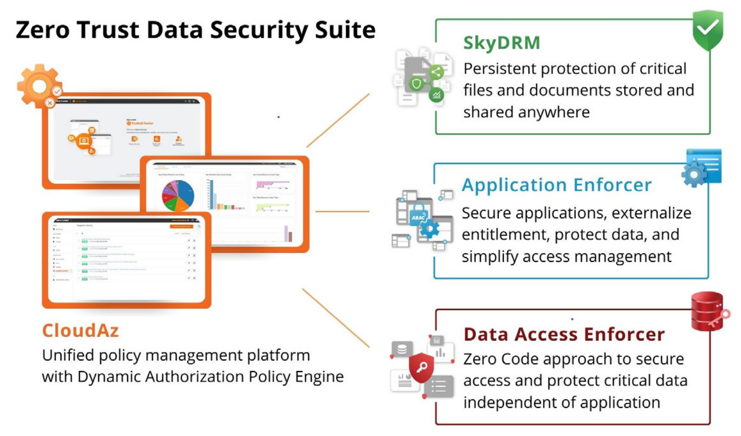
NEXTLABS DATA PROTECTION™

Data Protection is a host-based data loss prevention (DLP) product that automates active controls to streamline compliance and prevent data loss on endpoints, servers and mobile devices. Companies can now achieve continuous compliance with regulation, prevent data loss, and mitigate insider risk, and preserve data confidentiality across the global supply chain.

NEXTLABS® | Zero Trust Data-Centric Security

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**.



Zero Trust Data Security Suite

SkyDRM
Persistent protection of critical files and documents stored and shared anywhere

Application Enforcer
Secure applications, externalize entitlement, protect data, and simplify access management

Data Access Enforcer
Zero Code approach to secure access and protect critical data independent of application

CloudAz
Unified policy management platform with Dynamic Authorization Policy Engine