Solution Brief

Financial Services

Information Risk Management Solutions to Automate Audit & Compliance, Centralize Entitlements Management, Enforce Information Barriers across Communication Channels, and Protect Data

FINANCIAL SERVICES AND APPLICATIONS

Audit & Compliance
Discover and classify unstructured data to identify access and usage risks

Enterprise Application Enforcer
Centrally configure, administer, enforce, review, and audit fine-grained access policies and authorizations to mitigate unauthorized access, simplify audit, and improve compliance

Information Barriers
Protect communication and collaboration to prevent conflicts of interest and avoid regulatory violations

Data Protection and Rights Management
Protect data at the end point, and control usage inside and outside the enterprise

INFORMATION RISK MANAGEMENT CHALLENGES

Companies in financial services, such as those in insurance and investment services, are under intense scrutiny due to high-profile cases of improper data disclosure, including analyst research shared with bankers, client deals disclosed between internal teams, and confidential client data misdirected via e-mail to unauthorized recipients. Moreover, the inability to centrally manage a consistent set of policies across data to control unauthorized access and use, and a lack of comprehensive auditing, has led to increasing risk exposure.

SEC, NASD and NYSE regulations, BSA, and Sarbanes-Oxley rules, require strict enforcement of boundaries to preserve data confidentiality. GLBA, CA SB 1386, and similar mandates also require personally identifiable information (PII) to be kept private. With non-compliance penalties and loss of revenue including regulatory fines, legal liability from clients and shareholders, and loss of brand value, financial services organizations must actively control the loss of material non-public data to limit risks.

Unfortunately, today's silo solutions and system-specific controls do little to protect data once exported from repositories, nor do access controls understand the context of how data should be handled and disclosed properly across complex organizations. Gaining comprehensive visibility into data loss, and automating and maintaining a single set of top-down policies that maintain information confidentiality, are essential to improve compliance and mitigate risk.

THE SOLUTION

The Solution includes key applications for material non-public information audit and compliance, conflict and disclosure management, centralized entitlements management, and enforcement of controls to prevent inappropriate data access and conflicts of interest. Financial services companies can now comply with industry regulations, control access and usage of data, and simplify audit by centrally managing information use activities, implementing entitlements—and putting in place information barriers, document handling workflow, and disclosure policies—for material nonpublic information.

Identity and Solutions

The Solution addresses requirements for the discovery, access control, handling and protection of data. It integrates with and leverages existing infrastructure to apply identity-driven policies across users and resources. Identity-driven policies understand user context and environment variables during enforcement. Financial services companies can:

- Identify material non-public information
- Centrally define authorized users and proper entitlements
- Control data access, use, disclosure, and information barriers across the enterprise
- Align controls with corresponding business policies, regulatory rules, and contractual obligations
- Provide a full audit trail of data flow history and user activity to satisfy internal and regulatory compliance requirements.

KEY APPLICATIONS

The Solution includes four (4) key applications to address information risk management problems and workflow scenarios that are specific to financial services companies.

Audit and Compliance

Gain visibility and understanding of the location, access rights, use, and distribution of material non-public information. Reporting and analytical capabilities provide:

- **Inventory details** – centrally aggregates information on "what, where and who" by identifying material non-public information, its location, and the rights associated with its use
- **Entitlement audits** – reports and audits access rights for material nonpublic information, and analyzes if access rights are properly granted
- **Activity audits and compliance monitoring** – provides run-time inspection of user activity throughout the material non-public information lifecycle.

Ease audits, improve compliance, accelerate conflict and disclosure analysis, and proactively impelement information compliance.

Enterprise Entitlements Management

Centrally configure, administer, enforce, review, and audit fine-grained access policies and authorizations. Standardizes the management of entitlements across unstructured data repositories to reduce the cost of administration; simplify the audit of authorizations for compliance; and enable IT to implement fine-grained access control across applications quickly to react to business change, regulations, or legal inquiry.

Information Barriers

Comply with industry regulations by auditing and enforcing boundaries during communications and collaboration. Identity driven policies prevent information sharing between groups of users by requiring the proper use of confidential data to avoid violations.

Data Protection & Rights Management

Information on desktops or mobile devices is easily leaked when copied to removable media, uploaded or copied to unsafe areas such as unsecured FTP, or misdirected via e-mail to wrong recipients. It is important to control access and usage of material non-public data inside and outside the enterprise network, while educating users of appropriate use policies, and automating document workflow and remediation procedures to eliminate user errors.

SOLUTION DEPLOYMENT

NextLabs utilizes a combination of compliance and security expertise, industry best practices, and proven services and implementation methodology to deliver a solution built on its leading information risk management software. The deployment process includes:

Step 1: Monitor, record, and analyze information handling activities to discover and identify the risks of data loss.

Step 2: Author, manage, and deploy policies based on XACML, an industry standard, to achieve information compliance and data protection controls across applications and communication channels.

Step 3: Apply controls to educate users about policies and procedures; automate workflow and remediation to improve data handling; or block activities or alert policy stakeholders.

Step 4: Measure the effectiveness of information compliance and protection controls with reporting, continuous audit, and compliance analysis.

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**.