Solution Brief

Information Barriers Management

Monitor and actively enforce boundaries between internal organizations to avoid conflicts of interest when data is accessed and disclosed improperly

OVERVIEW

Industry and government regulations require strict enforcement of barriers that preserve confidentiality when handling sensitive data, such as material information. For financial services and similarly regulated companies operating in a globalized environment, these barriers can include:

Regulatory: SEC - Research and investment banking barriers to prevent conflict of interest

International: EU Directive on Data Protection - Prohibiting the transfer of personal data to non-European Union nations that do not meet "adequate" standards for privacy protection

Entity: Japanese Privacy Law - Rules regarding third-party transfer or disclosure of personal information without prior consent

SOLUTION HIGHLIGHTS

A single policy to maintain information barriers
Improve efficiency and reduce errors across multiple points where data is communicated, distributed, and stored.

Policies codified and automated electronically
Enforce compliance procedures in less time and with less cost

Real-time controls
Apply context including identity, data types and activities, and business conditions for fine-grain definition of barriers

User education and procedure automation to prevent violations
Train and assist users to handle data properly, and avoid indiscretion or unintended misuse

Comprehensive auditing and reporting
Monitor activities, discover risks, and remediate gaps to prove compliance

Similar regulatory mandates further require organizations to responsibly manage the disclosure of client nonpublic personal information (NPI) and personally identifiable information (PII), or face consequences. With noncompliance penalties that include regulatory fines, legal liability from clients and shareholders, and loss of brand value, companies must actively monitor and control the use of sensitive data across organizations to limit risks, and prove compliance with policies.

But today's siloed solution approaches do little to maintain boundaries, once information is transferred from controlled applications and systems. Moreover, today's coarse-grained controls lack the sophistication and deep identity awareness to discern organizational relationships and proper information sharing activities that would define safe disclosure.

THE SOLUTION

The enterprise can now enforce proper information access entitlements and handling policies with controls that create and maintain barriers across complex organizations. The Information Barriers Solution allows companies to:

- Create boundaries that reflect business relationships based on regulatory, international, or entity requirements
- Manage data access, handling, and disclosure with consistency across communication and collaboration channels to prevent improper activities, while remaining transparent to normal business
- Educate users about policies and procedures to increase compliance awareness
- Monitor activities comprehensively (surveillance), simplify auditing, and report violation attempts to prove effective policy.

The solution helps companies to automate the enforcement of information sharing and communication compliance procedures by rapidly creating information barriers across teams, departments, business units, entities, subsidiaries, regional locations, and resources. Consistent controls are enforced at applications, desktops, and servers where data is stored, shared, and distributed to prevent conflicts of interest and improve corporate integrity.

BARRIERS THAT UNDERSTAND THE BUSINESS CONTEXT

Managing disclosure is difficult when devices, data, and users are mobile, or if users, customers, partners, and subsidiaries are spread across multiple locations. The Solution allows information barriers to be described using context—such as identity, data type and activities, and business conditions—to align with regulatory policy definition.

The Solution includes:

E-Mail Barriers

The E-mail Barrier Solution provides controls across enterprise messaging clients to create a consistent boundary.

Unified Communications

Controls are provided across multi-channel communications to create a boundary that is consistent across voice and electronic communications applications (IM, e-mail, VoIP, Web conference, etc.).

Collaboration Barriers

Controls across collaboration portals, such as Microsoft Office SharePoint, create a virtual boundary when information is attempted to be shared or during improper access attempts.

File Sharing Barriers

Controls across Windows and Linux file shares, and Web or FTP servers, create a consistent boundary that limits disclosure.

SOLUTION DEPLOYMENT: HOW TO GET STARTED TODAY

NextLabs implements the solution by using expert product knowledge and a services best practices methodology. NextLabs can also assist clients with identifying their controlled data, 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 using Enterprise DLP™, along with any custom Policy Assistant automation.

Step 4: Install POLICY ENFORCERS
Policy Enforcers are deployed across applications and systems, if applicable to requirements.

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**.