NEXTLABS®

White Paper

Data-Centric Security for the Extended Enterprise

Four Ways It Must Change

Yesterday's security is no match for the challenge of protecting data across the extended enterprise, with sensitive data increasingly shared across organizations, over external systems, and with unknown users and devices.

A basic shift towards data-centric thinking must replace conventional device- and container-based models. But where do organizations start? What assumptions must change?

This white paper outlines four changes organizations must make to achieve data-centric security, and explains why IT Leaders, Security Professionals, and Compliance Officers should care. This paper then provides a brief overview of the NextLabs approach to Information Risk Management.

"...IT must retain visibility and control access across the extended enterprise, regardless of location, device, user population, or hosting model."

--Forrester

INTRODUCTION

The extended enterprise is the new normal. The limitations of enterprise authorization management are quickly becoming obvious with the revolution in information sharing, cloud computing, and mobility. In most large enterprises, security professionals already grapple with uncoordinated information infrastructure and a patchwork of disparate security systems. But now the "extended enterprise"— what Forrester describes as an "ecosystem of customers, devices, clouds, service providers, partners, supply chains, and empowered users"—is highlighting the fundamental weaknesses of traditional identity and access management.

In the extended enterprise the only thing you control is data. Conventional security approaches were never designed to accommodate the extended enterprise. The fundamental assumptions of ownership and trust have been violated. Network perimeter controls, organizational roles, user account management, and endpoint security assume that the organization owns the infrastructure and applications and trusts the devices and users. Yet, the Cloud, SaaS, BYOD, outsourcing, and insider data breaches invalidate all of these assumptions.

Why try to Protect What You Don't Control?

In the extended enterprise, controls must be able to protect data even when organizations cannot...

- Own relevant data "containers" (on systems, devices, network locations, applications, and so on)
- Identify all authorized users and devices
  Enumerate a set of rules ahead-of-time to cover all scenarios of data access

When the only thing an organization reliably owns is data, device- and infrastructure-centric concepts like trust must be replaced with data-centric strategies for managing risk.

Where to Start?

Unfortunately, the current IT reality is more complicated. While a fundamental shift is required, it cannot happen overnight. We still have hundreds of applications and business processes to maintain. IT must start planning its strategy to extend responsibilities from securing infrastructure and managing users, to securing data and managing information risk:

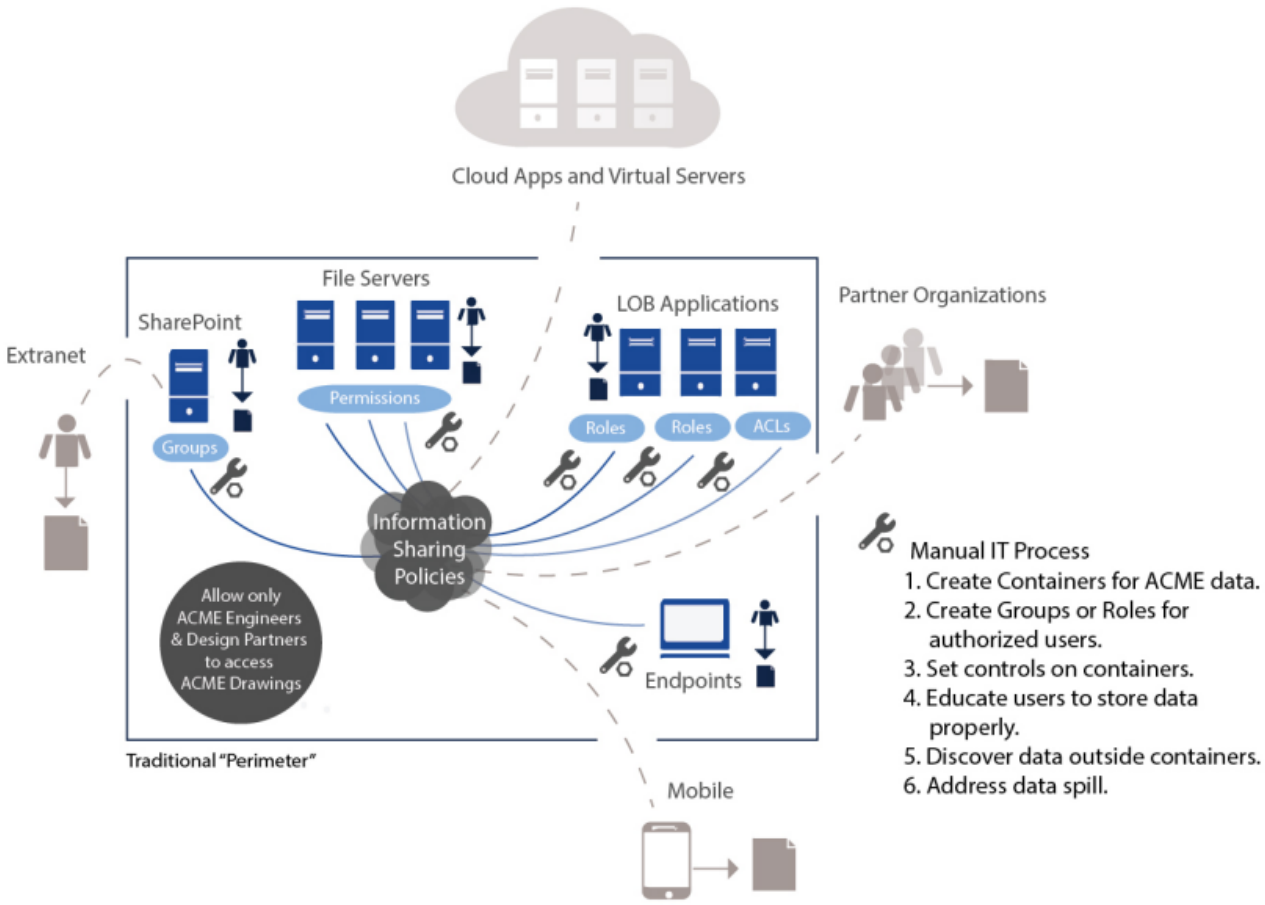
- How can security controls be applied to data regardless of application, infrastructure, or device?
- Information risk is dynamic, that is, it changes based on a number of contextual factors. How can controls determine and adapt to risk before providing access?

LIMITATIONS OF TRADITIONAL CONTROLS

Permissions, Access Control Lists (ACLs) and Roles are neither data-centric nor risk-aware. They are applied to containers (e.g., folders), applications, and services. Once data leaves a container, the data is unprotected.

In terms of implementation and maintenance, traditional controls require IT to manually translate information sharing policies into system-specific controls, then duplicate work across all applications and systems where sensitive data moves. Because controls are static, administrators must also modify and re-assign them as risk, workflow, or personnel change.

In a large enterprise, IT process quickly becomes inefficient and error-prone. In the extended enterprise, where data sharing is broader than ever and organizations no longer reliably own infrastructure, this approach is often impossible.



ATTRIBUTE BASED ACCESS CONTROL FOR DATA-CENTRIC SECURITY

Organizations implement Attribute Based Access Control (ABAC) because they acknowledge traditional access control is not adequate. ABAC provides a dynamic way to turn business rules into security controls structured explicitly around attributes of data that reflect business value. Rather than protecting data indirectly--that is, by applying controls to the **container** where data is stored, or to the device or applications used to access data--you design controls around the **characteristics of data that warrant protection in the first place.** This could be content, team ownership, security clearance level, and so on. Because regulations and corporate policies are generally written around these attributes, ABAC maps the same business concepts embedded in an information control policy to digital attributes for users, resources, and context.

ABAC eliminates the manual steps required to turn business rules into security controls. Unlike traditional controls, which require permissions to be defined statically before an access attempt occurs, ABAC rules are evaluated dynamically with attributes presented at run-time. Enforcement adapts to risk level automatically. For example, if the classification of a document changes, or a user's team membership changes, access rights are automatically adjusted. No need to request new roles or update permissions.

Challenges to Implementing ABAC

If ABAC is so game-changing, why isn't it more broadly adopted? On its own, ABAC is not sufficient to address data-centric security. ABAC requires appropriate inputs to work. For data-centric use cases, we need three critical inputs: data classification, identity attributes, and policy.

It sounds easy, but most organizations do not have the responsibilities and processes in place to provide these inputs. Before the potential benefits of ABAC can be realized, the IT mind-set needs to change from protecting devices and applying static concepts like trust, to setting up systems that make inputs available for dynamic access controls.

INFORMATION RISK MANAGEMENT

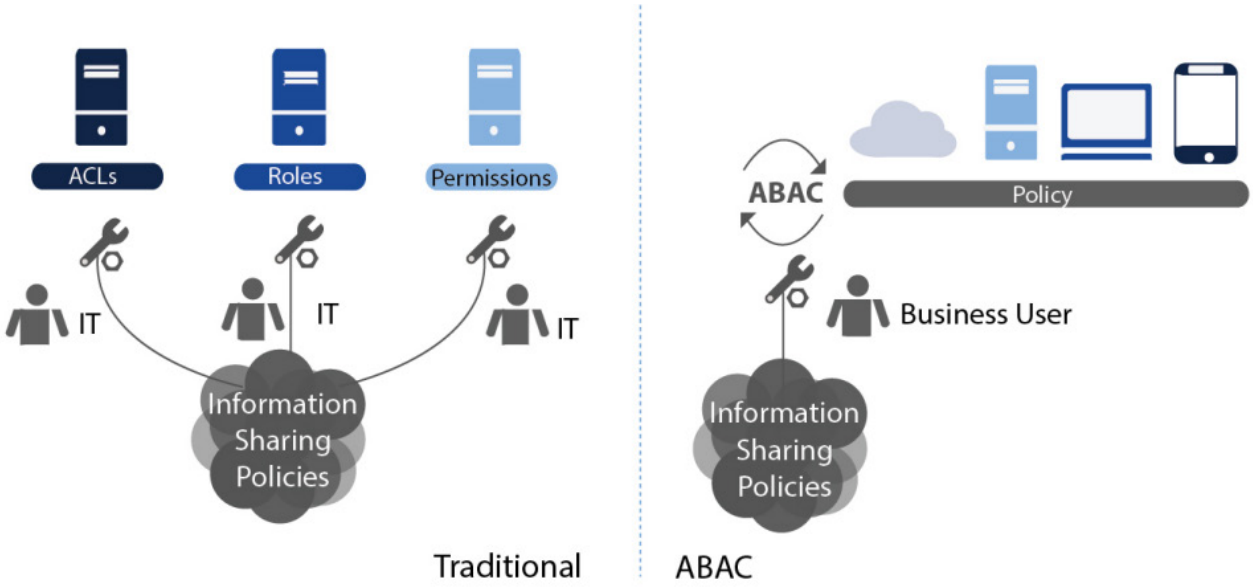
Information Risk Management is an integrated solution that enables companies to leverage ABAC for data-centric security use cases. By providing integrated services and tools for data classification, identity integration, business policy management, and data protection Information Risk Management enables four fundamental shifts in IT process:

- Define business policies, not permissions.
- Manage attributes, not user groups.
- Control access to information, rather than securing containers.
- Make it easy for end users.

Data-centric IT protections should digitize business requirements as they are already written.

Define Business Policies, Not Permissions.

With Information Risk Management, controls transparently reflect business requirements with no need for translation into system-specific frameworks such as permissions, roles, or ACLs. Information Risk Management policies digitize business requirements as they are written. A single policy, expressed in business terms, is applied cross-system. IT no longer acts as the "middle-man" between compliance officers and data owners and the physical systems where data is stored.

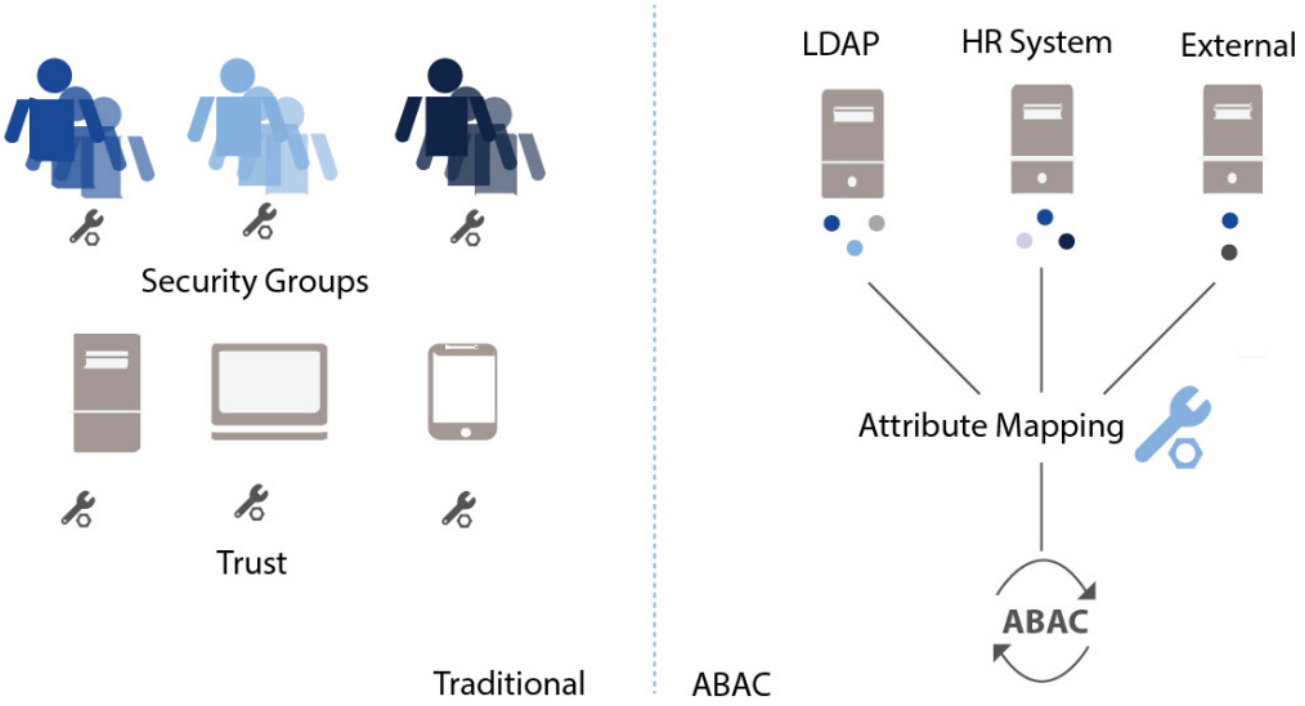


Manage Identity Attributes, Not User Groups

The real challenge in identity management is the lack of ownership, accuracy, and centralization of identity attributes.

Most IT environments already contain digital attributes for data, users, devices, locations, and applications. This information is stored in disparate locations: Active Directory or LDAP, file properties and metadata, roles and enterprise applications.. The problem is not a lack of available attributes, but unclear ownership, responsibility for their accuracy, and no means to leverage them for consistent enterprise-wide policy evaluation.

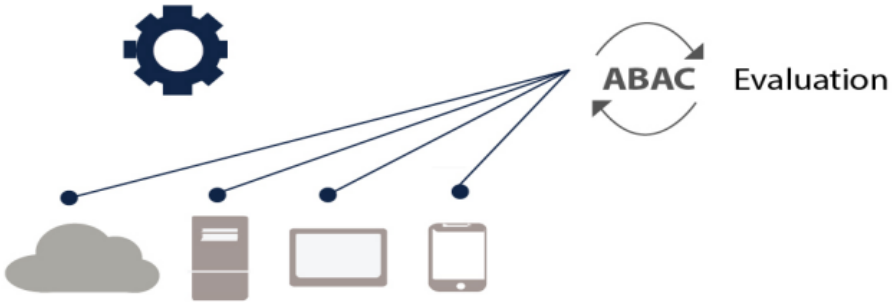
The IT function shifts from administering security groups, to implementing automated processes that enable attribute owners to maintain this critical information. In this model, some attribute stores may be “owned” by IT (such as Active Directory), but many may be owned by other teams or even managed outside the enterprise.



Control Access To Information, Rather Than Securing Containers

With Information Risk Management, when a user attempts to access information, location or container is just one attribute that can be collected and evaluated. You don't have to use container-based controls as the only means to protect data, but can incorporate more data-centric controls that target metadata, keywords, properties, and so on. Because evaluation is based on attributes of the data, controls apply consistently as data moves between containers and across systems.

Container-based controls never apply consistently to data across systems.. Information access events must be the explicit target.



Make It Easy For End Users

An Information Risk Management solution can provide automated services so business users drive data protection. For example, data owners can be responsible for creating and applying data attributes, which makes sense, since they are typically most familiar with data and information sharing requirements. Once data is classified, data attributes drive automated controls (such as encryption, storage and access controls, and so on). Or, in a fully automated workflow, the attributes of a file (metadata, storage location, content, file property, and so on), drive how the file is classified and controlled.

Automation enables users outside of IT to manage information risk.

NEXTLABS INFORMATION RISK MANAGEMENT: CONTROL CENTER

NextLabs Control Center is an Information Risk Management solution that allows organizations to centrally administer, deploy, and enforce information control policies. Business users are empowered to define fine-grained, data-centric controls thanks to critical automated services that are coordinated across the extended enterprise.

Business Policy Management

With Control Center, business policies are digital versions of your information sharing requirements. Business policies are centrally managed in a common language and deployed cross-system. Business Policy Management enables organizations to apply one set of business policies, rather than "translate" information sharing requirements multiple times into permissions, roles, and ACLs.

Attribute Management

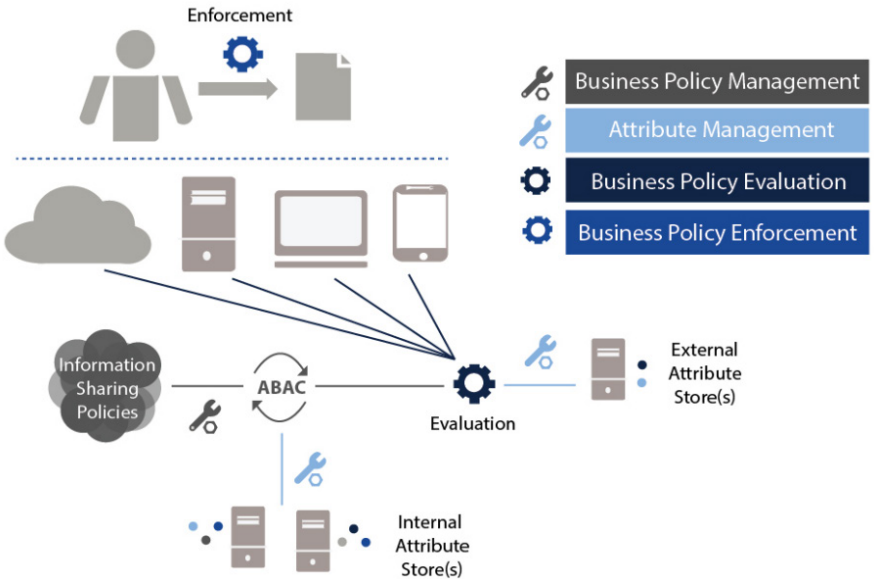
Attribute Management allows organizations to leverage attributes already available, both internally and externally, for consistent policy enforcement across the Extended Enterprise. Attributes available in disparate identity stores can be owned and administered by different teams (both internally and externally), at the same time as being centrally integrated with Control Center so they are available during policy evaluation.

Business Policy Evaluation

In the Extended Enterprise, policy evaluation must be applied to data, no matter where it resides: on desktops, servers, the cloud. Control Center's Business Policy Evaluation provides data-centric evaluation.

Business Policy Enforcement

Wherever possible, automation should make information risk management easy for users: data owners, end users, auditors, and troubleshooters. Business Policy Enforcement supplies automated services that replace the standard manual work of data centric security.



Wherever possible, automation should make information risk management easy for users: data owners, end users, auditors, and troubleshooters. Business Policy Enforcement supplies automated services that replace the standard manual work of data centric security.

Extending It With Control Center

Control Center allows organizations to implement data-centric information controls and streamline and extend traditional IT security efforts. Control Center transforms how IT manages three critical inputs for Information Risk Management: Policy, Identity, and Data.

Inputs	Traditional Security	Information Risk Management
Business Policy Implementation	**Application Developer (IT):** Translate business requirements into technical controls across owned and virtual systems, including specialized cloud security applications and third party service providers	**Policy Author:** Digitize business policy into one set of controls
Identity Management	**Identity Management (IT):** User Provisioning and Security Groups for internal users; no capabilities for external or unknown users IT Helpdesk: Managing user group members.	**Identity Management (IT):** Set up integrations with physical systems where identity attributes are stored. Systems can be internal or external. **Attribute Owners:** Maintain attribute information for users; attribute owners can be internal (HR, IT, GRC) or external.
Data Management	None: There are no capabilities for data management in traditional security systems; IT must attempt to protect data by securing container	Data Owner: Apply metadata to files based on the business value of data

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.