NEXTLABS®

White Paper

Addressing Gaps in Your Cyber Security

Solution Design at the Data Layer

Because the biggest impact of cyber breach is data loss, data protection should be architected into the DNA of your cyber security solution. This means focusing security efforts around data from the very beginning, from initial risk assessment, to control design, to implementation and auditing.

Most cyber security solutions protect infrastructure, assuming that data stored within containers will be protected. This white paper explains why this assumption is no longer valid and outlines an approach to designing a cyber security solution directly around data.

Compliance Officers, Risk Managers, Security Professionals, and IT Leaders will understand the goals and steps of data-centric solution design, as well as its potential benefits.

INTRODUCTION

How can an organization extend data protection beyond the container?

With cyber threats on the rise, the biggest gap in your cyber security solution is most likely data protection. Conventional IT tools protect information by securing infrastructure from external attack and applying controls to “containers.” However, the biggest source of cyber threat is increasingly “business as usual,” that is, authorized users sharing sensitive data, increasingly outside controlled locations.

Across every industry, business process is becoming more globalized, devices are proliferating, and new data storage and hosting models continue to emerge. Data is being shared more broadly than ever, and infrastructure-based IT controls simply cannot keep pace.

Organizations are recognizing the need to go beyond infrastructure-centric controls to protect data directly, regardless of system, device, or application, and whether data is inside or outside the "traditional" perimeter. This is especially true for data that warrants extra protection, such as highly sensitive data or data regularly shared with external partners and organizations. What would it mean to design a cyber security solution to protect data based on business value and risk? How would an organization extend data protection beyond the container?

This white paper presents an approach to solution design that takes data as its starting point. The goal is precision: to target sensitive data, identify data sharing use cases where risk is high, then apply uniform controls to protect data, no matter the system, application, or device.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

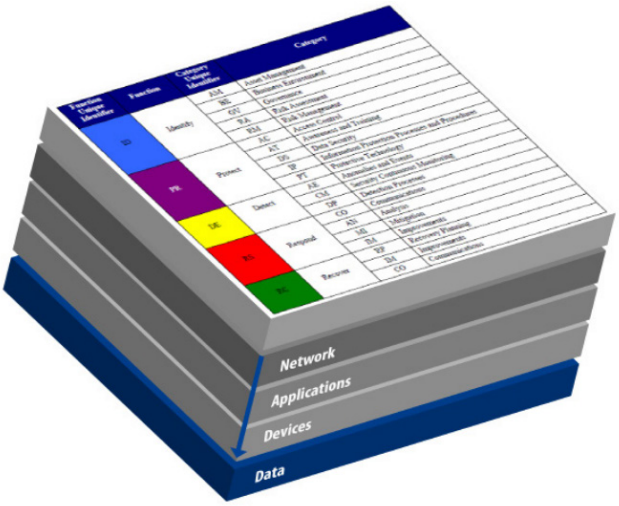
IMPLEMENTATION CHALLENGES: THE NIST EXAMPLE

Frameworks for cyber security, like the one supplied by the National Institute for Standards and Technology (NIST), attempt to provide a top-down view of the functions of a comprehensive cyber security solution.

In the early stages (the "Identify function," in the NIST framework), Risk Assessors identify Vulnerabilities—meaning potential system weaknesses that can result in cyber breach. In the "Protect" function, these Vulnerabilities are translated into technical protections.

After this "translation" process, an organization may not even know if vulnerabilities identified in the early stages of solution planning are even addressed at all. Different teams are typically responsible for applying controls to different systems. There is rarely any coordination or visibility into how different teams apply technical protections across layers of architecture.

In this approach, the lowest layer of protection (data) is assumed, rather than explicit. While initial vulnerabilities may be expressed in terms of data loss and leakage, protections themselves are not designed around data. None of the IT protections (trusted devices, application-specific ACLs, rules, and permissions), protect data directly.



The result of these challenges is that data protections may or may not be "translated" adequately into system controls, and protection may not persist as data leaves the container.

One way to address these challenges is to understand the work that needs to occur in between the "Identify" and "Protect" functions of frameworks like NIST. An organization must have a method to:

- Track how initial data protection requirements are translated into technical controls
- Ensure protections are implemented consistently cross-system.

Standard solution design ends with containers. Data-centered solution design starts with data itself.

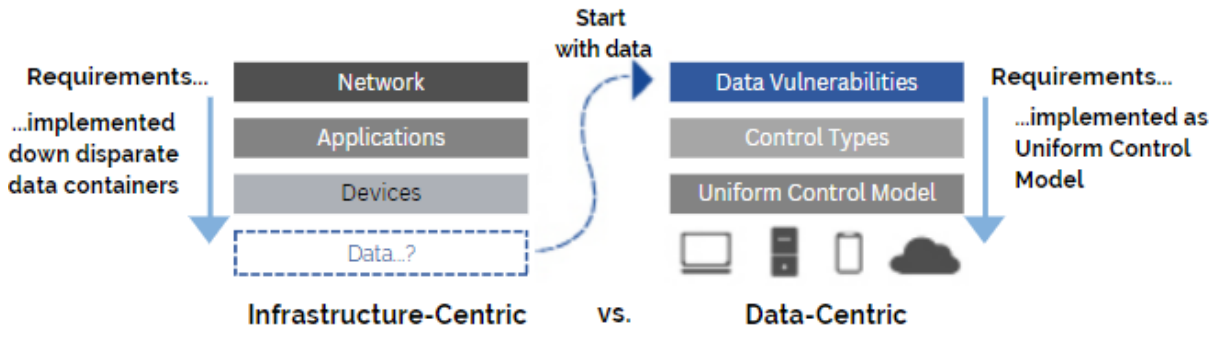
USING A UNIFORM CONTROL MODEL

Developing a Uniform Control Model for data-centric security inverts the process of standard, infrastructure-centric security design.

The standard process translates initial requirements into technical protections at various layers or architecture, assuming data underneath each layer will be protected.

In contrast, a data-centered design starts with data itself. First, Data Vulnerabilities--which are data-related events that can result in cyber breach--are identified within a structured framework. Importantly, Data Vulnerabilities are not defined in terms of system weaknesses, flaws, or external attacks--but in terms of regular events that occur during "business as usual" data access, usage, and sharing. You then map each Data Vulnerability to a Control Type. Together, all the controls form the Uniform Control Model. Because there is a clear mapping from Data Vulnerability to Control Type in this method, there is better visibility into how each data protection requirement is being addressed.

The Uniform Control Model is system-agnostic, meaning that while systems may be referenced in controls (file servers, line of business applications, and devices where data is stored), controls are not written in the proprietary logic of a particular application or system (for example, ACLs or permissions on file servers). The goal is to produce a highly auditable, centrally managed set of data controls that can be deployed cross-system.



Step-by-Step

Perform the following three basic steps to produce a Uniform Control Model for data-centric cyber security:

1. Identify a set of data under threat, where the business value of the data warrants controls.
2. Identify specific Data Vulnerabilities as data moves through its standard process: creation, access, usage, and sharing.
3. Map each Data Vulnerability to a specific Control Type in the Uniform Control Model.

The following sections describe these steps in more detail using a Uniform Control Model produced by NextLabs. This model accumulates standard data protection technologies and incorporates them into a comprehensive control framework.

The key for data-centric security: the level of protection should match the value of data and degree of risk.

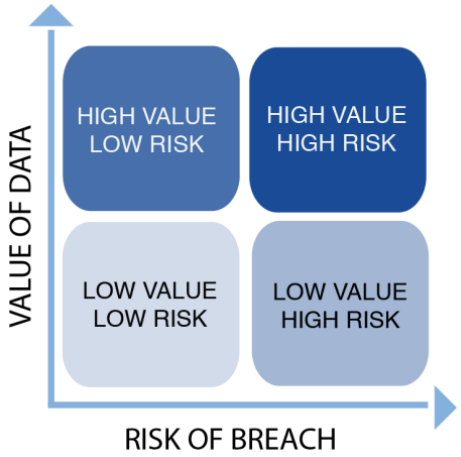
STEP 1. TARGET DATA BASED ON BUSINESS VALUE AND RISK

When organizations attempt to design data-centric controls, they confront a sea of data, complex data sharing practices, over uncontrolled devices, and even with unknown users. Where to begin?
The answer is simple: start small.
Target a class of data that has high business value and is highly susceptible to cyber breach. A key guideline for data-centric protection: the level of protection should correspond to the business value of data and degree of risk.
For much data, traditional, infrastructure-based controls may suffice. For highly sensitive and valuable data and/or data that is unusually susceptible to cyber breach, a data-level solution is likely warranted.

Example: Project Catalina

Consider the following scenario: a high tech design firm regularly shares data with multiple external partners. The most sensitive project, Project Catalina, includes multiple contract design firms who collaborate
on design drawings for a new product. For successful collaboration, the company must regularly share proprietary design drawings with outside contractors (many of whom also contract with competitors).

This scenario is an ideal candidate for a data-level solution. It involves a identifiable class of data that is both high in business value and highly susceptible to loss or leakage. It also involves a business initiative that is high priority for an organization, but also introduces new forms of information risk.



STEP 2. IDENTIFY DATA VULNERABILITIES

As mentioned above, "Data Vulnerabilities" are data access, usage, handling, and sharing events that can potentially result in cyber breach. This following table list the most common data vulnerabilities with examples for Project Catalina.

Vulnerability Type	Description	Examples (Project Catalina)
Classification	Data improperly classified	Project Catalina Design drawings not classified or mis-classified
Storage	Data stored in improper locations	Project Catalina Design drawings stored in insecure location on user PC or collaboration server
Access	Data access granted to unauthorized users, or access denied to authorized users	Project Catalina Design drawings accessed by non-Catalina Team member in collaboration server
Usage	Data handled, used, or distributed improperly	Project Catalina Design drawings moved to insecure location, content modified (copied and pasted into new document)
Communication	Data shared over communication channels with unauthorized users, or shared over unauthorized (uncontrolled) channels	Project Catalina Design drawings emailed to non-Catalina Team member Project Catalina Design drawings emailed over unauthorized channel
Visibility	Limited or lack of visibility into how data is managed, used and shared	Limited or no visibility into classification, storage, access, usage, and communication events

STEP 3. APPLY CONTROL MODEL

Because Data Vulnerabilities are organized in a structured framework, they can easily be mapped to Control Types. A "Control Type" refers to a class of controls for protecting data. For example, "Data Classification" is a Control Type, which can include several different controls (automatic content scanning, tagging, watermarking). Controls can be discretionary or mandatory, manual or automated, and implemented using a variety of methods and technical solutions.

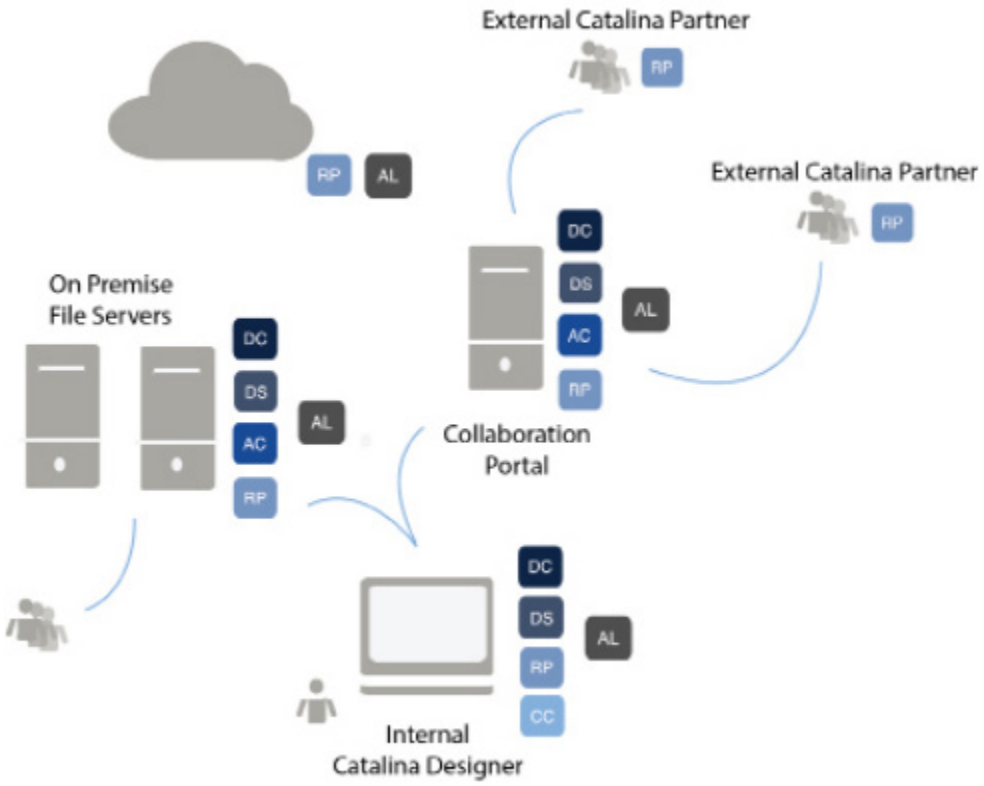
	Control Type	Description	Examples (Project Catalina)
DC	Data Classification	Scans data to evaluate content or another property Applies tags to data Applies visual labels to document data and applications	DC_1. Require internal Project Catalina content owners to classify new Project Catalina design drawings. DC_2. Automatically scan content and classify Project Catalina design drawings uploaded to collaboration portals and file servers or emailed.
DS	Data Segregation	Prevents a class of data from being stored in an unauthorized location Restricts storage of a class of data to a secure location	DS_1. Restrict storage of Project Catalina design drawings outside My Documents folder on PCs DS_2. Restrict storage of Project Catalina design drawings outside Project Catalina Team Site in collaboration portal and secure file server location
AC	Access Control	Controls access to resources, including opening, renaming, changing permissions or attributes, or deleting a resource	AC_1. Restrict access of Project Catalina design drawings to internal Catalina team members and external Catalina Partners in collaboration portal and file servers.
RP	Rights Protection	Controls data-level usage, including printing, deleting, copying, saving, and modifying	RP_1. Automatically apply rights protection to Projection Catalina data. RP_2. Restrict to "view only" access for Rights Protected Project Catalina design drawings, except for content owner team
CC	Communication Control	Controls the distribution of data through communication applications	CC_1. Prevent email of Project Catalina design drawings to non-Project Catalina users CC_2. Prevent sharing of Project Catalina design drawings over unauthorized channels
AL	Activity Logging	Monitors data access and usage	AL_1. Monitor classification, storage, access, usage, and communications events for Project Catalina design data across file servers, collaboration portals, and endpoints

=

The end product of this design work is a comprehensive list of Control requirements. The next step is to design the technical solution to implement these controls. Organizations typically use a blend of approaches, including manual procedures, user education, administrative processes (email alerts and work flows), and where possible, control automation.

While there are many options for automation, an ideal technical solution would support automation cross multiple systems. The same automation for Rights Protection, for example, should be available on file servers, endpoints, and so on. Another best practice is to use data-centric technical controls that target data by property and attribute (classification, content, and/or location) rather than just by container. That way, the same method used to target data (metadata tag, for instance) can be automated cross-system.

Finally, ideal technical controls are written in a language that mirrors—as closely as possible—the language of non-digital controls in the Uniform Control Model. This enables better visibility into how non-digital control requirements get implemented as technical controls.



CONCLUSION: BENEFITS OF DATA-CENTRIC SOLUTION DESIGN

While this white paper only covers the early design stages, the potential benefits of a data-centric approach to cyber security solution design should be clear.

Taking the time to derive a Uniform Control Model allows organizations to use a consistent vocabulary while defining controls. Controls can be re-used cross-system, for better consistency, as well as a clear audit trail. Auditors, troubleshooters, and compliance teams can track exactly how core Data Vulnerabilities are addressed.

While our example scenario in this white paper was a narrow use case, after successfully implementing one data-centric solution, most organizations will want to extend protections to other classes of data. The Uniform Control Model is inherently extensible and scalable.

Perhaps the biggest benefit of a data-centric orientation, however, is that data protection is built into the heart of your cyber security solution. Organizations apply the deepest level of controls to data that needs it most—the most sensitive, valuable, and vulnerable information—no matter where it resides.

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.