NEXTLABS®

White Paper

What Will Data-Centric Security Look Like Over the Next 5 Years

The NextLabs Solution Architecture

According to NIST Cybersecurity, confirming data-centric security is an important challenge to address over the next five years with an increased virtualization of the workforce in the post-COVID environment.

"Data safety" is the new data security

We've all heard about data security, but how many of us use the term "data safety?" "Data security" has been around for a long time, but we've entered a day and age where we need to start rethinking its relevance and how it needs to evolve to address the true needs of the hyper digital new world.

Let's start with a refresher on what "data security" is all about. It means protecting digital data, such as those in an application or file, from destructive forces and from the unwanted actions of unauthorized users, such as a cyberattack or data breach. However, the term often connotes locking down data such that it cannot be shared. Locking down data in the name of "data security" conflicts with the collaborative times in which we live and makes it more difficult for companies to achieve their strategic objectives. The acceleration of the digital economy, exponential data growth, the ubiquity of mobile devices, cloud computing, and globally dispersed organizations require the sharing of information with colleagues and partners without running afoul of the myriad security and compliance requirements your company is held to.

Enter **data safety** and the implementation of preventive controls to safeguard data that's being used and shared. Data safety essentially gives you the best of both worlds: the ability to share data with colleagues and partners without sacrificing data security.

How is this done? The most effective way to safeguard data is to incorporate and automate data security controls into key business processes. These would be things like:

- Understanding what kind of data you've got and where it's stored
- Understanding how it's being used and by whom
- Establishing policies, controls, and a governance model with built-in auditing
- Implementing the proper level of data protection (think "preventive" instead of "detect and mitigate")
- It is difficult to identify all authorized users and devices
- Reporting and auditing to prove how the data is used, who uses it, and for what purpose

1. Applications run the business

A simple glance at your smartphone and you'll quickly notice how much applications consume our daily lives. From Gmail to LinkedIn to Uber, we need these applications to stay in touch with family and friends and to remain productive. From a business standpoint, applications like ERP, CRM, and PLM are the equivalent applications that keeps your business humming and remaining relevant in an increasingly competitive global economy.
Because applications drive much of the business these days, most, if not all, of the business-critical data are generated and managed by applications. Thus, it's crucial to understand the different classes of data and what value they bring to the table. Once you have a sense of your data, then you can implement the appropriate controls to ensure that the high-value and high- risk data stays safe while being made available to the relevant stakeholders. If you protect data at the source (i.e., within the application) and with the right controls in place, you put yourself in a position to extend that protection as the data flows from one application to another – all with using a consistent set of policies. Protecting data at the source is prudent as the potential problems increase exponentially when the data flows downstream (i.e., as it is shared and reshared with ever more users).

2. Applications are the engine for data classification

Applications generate 80% of the business-critical data that end up in unstructured data environments. The key, however, is capitalizing on the metadata in the applications to tag and classify data as it moves into the unstructured world. Whether it's a Word doc, a PowerPoint file, or a PDF, these are all examples of unstructured data getting shared internally or externally. Thus, fundamental to any sound data security strategy is the establishment of a consistent, repeatable approach to classify data automatically by leveraging and reusing the metadata from where data originates – the applications.

That's why data and applications are so intertwined these days. To achieve "data safety," you have to understand the applications themselves (how they're structured, what metadata is available, how they're being used by the business, etc.) so you can design a data safety program that can scale and extend across the structured and unstructured data environments.

3. Data authenticity and accuracy

Digital data is presumed to be authentic if it can be shown that it was not corrupted after its creation. Data authenticity also means that a digital object is indeed what it claims to be or what it is claimed to be. With the explosion of data that the digital world has created, we've really got more content than we know what to do with — and we also often have trouble separating fact from fiction.

In fact, it's the company's responsibility to establish operating procedures that ensure the authenticity of their high-value, high-risk data. It's not a stretch to expect search engines, media outlets, and even social media to start cracking down on unverified data or unsubstantiated claims.

In other words, data authenticity will play a larger role over the next decade. There are enterprise data logging tools available that can help ensure data authenticity. Additionally, the establishment of standard operating procedures around the tracking of data lineage, systems of record, and audits will foster an environment of best practices for data authenticity.

4. Identity and master data management will become essential to the digital core

Good data safety is highly dependent on a solid identity and master data management (MDM) foundation. These days, most organizations have an identity system in place, be that Active Directory or something else, which has a lot of metadata within them.

The other component you'll need is a well-designed MDM system. MDM enables organizations to create and use a "single version of the truth" of key data assets, such as product data, asset data, customer data, location data, etc. It also manages a consistent and uniform set of identifiers and extended attributes that describes the core entities of the enterprise, such as customers, prospects, citizens, employees, suppliers, locations, products, projects, organizational hierarchies, and chart of accounts.

The net net is that you need an identity management system to provide metadata on the user, but you also need a MDM system to provide the metadata on all the other key attributes such as products, assets, customers, vendors, locations, etc. It's really a situation of the sum being greater than the parts: identity and master data management are more valuable together than independently. If the metadata is used prudently (and assuming that the metadata comes from trustworthy sources), then you're off to a good start for building a powerful policy management platform.

5. Secure data no matter where it goes

Most enterprises fail to properly safeguard business-critical data (beyond what's provided natively by the applications), leaving the data vulnerable to breaches and/or improper use. Permission to access data in the applications should not automatically allow the user to extract and share the data from applications freely. Ideally, you want to have the same safeguards and security controls on the data whether it's in the application or when it's taken out of the application.

By applying persistent security controls on the data via Enterprise DRM (EDRM) technology, you'll be able to protect your sensitive or confidential data no matter where it resides or goes. EDRM can be applied in such a way that as critical data is being removed or extracted from the application, the resulting files are protected automatically with policy to eliminate security airgaps where file is often left without proper protection and control in place.

Company should invest in policy-driven information control frameworks to automate information handling, data compliance, and information security procedures and ensure a consistent set of policies are applied regardless of where the data resides (i.e., whether it's stored in the application or when shared outside of the application). The net result is that you get peace of mind knowing that your critical data stays protected whether it's stored in the application or when it is shared externally via file or store in cloud storage.

6. Corporate governance and accountability will become more critical

Compliance has always been a mainstay for organizations, but going forward, we'll see corporate governance and accountability play more pivotal roles. Given that more regulations and industry guidelines are on the horizon, non-compliance and the lack of accountability will threaten a company's long-term survival more so than ever.

Whether it's SOX, SEC, HIPAA, export controls, etc., compliance requirements won't be going away any time soon. In fact, we're likely to see more regulations like GDPR pop up as data and privacy concerns become more entrenched in our daily professional and personal lives.

What this means is that monitoring and protecting your data as it's being shared is a best practice for responsible corporate governance and accountability. Falling short of this increases the likelihood of non-compliance and possibly financial penalties – not to mention the negative publicity, stock price volatility, and stalled strategic initiatives as a result of poor corporate governance.

Ultimately, it all comes down to preventing wrongful disclosure and safeguarding information sharing – effectively affirming the importance of data safety.

7. Hybrid cloud and multi-cloud are becoming the norm

Public and private clouds have increasingly dominated the computing landscape over the last ten years. However, due to the complexity of many enterprises' IT infrastructures and the varying security and compliance requirements, the need for hybrid or multi-clouds has jumped to the fore.

Why is this the case? One of the main reasons is the sharp increase in the number of applications moving to the cloud as a result of the shortcomings of the network-centric model. Trusting all users who are granted access to the network (and thus access to the applications) simply is not viable anymore given the ubiquitous nature of the cloud and what that entails (e.g., array of devices, access points, stolen credentials, etc.).

This has led to the emergence of the Zero Trust model whereby the focus shifts to protecting sensitive data stores, applications, systems, and networks themselves, instead of focusing on the perimeter. The model essentially protects data from the inside out, directly safeguarding a company's most prized assets.

Due to the widespread adoption of public cloud (i.e., IaaS) platforms, organizations are customizing platforms like AWS and Azure by creating private clouds on these IaaS platforms. These companies are deploying their own software and customizing their technology stacks with their own internal processes in order to push the innovation envelope.

Let's look at a scenario that requires a unique security approach to address multi-clouds. A European-based company might have a traditional on-premises ERP system on the backend, a virtual private cloud for application development hosted at AWS, and commercial SaaS applications to handle CRM and IT service management. But, being based in Europe, this same company has strict data residency requirements where data must be stored within national borders. Whereas this might not be feasible in a public-cloud-only environment, a hybrid infrastructure will certainly accommodate this type of requirement. From a data safety perspective, you need a standardized system to manage data access across all these different applications running on different platforms while considering the various data residency requirements, compliance mandates, and security standards the company must adhere to.

Tying it together

So, to bring this full circle, the trends outlined above point to a world where the next frontier of "data security" will be "data safety." It's a world predicated on sharing and collaboration with the requisite controls over that data to allow businesses to remain competitive and agile while ensuring safety and compliance mandates are met.

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.