NEXTLABS®

White Paper

Safeguarding Data in Joint Ventures, Mergers & Acquisitions, Divestitures, and Sanctions

INTRODUCTION

Safeguarding data should always be a concern for organizations, and certain situations can make this more challenging. One of the most challenging scenarios is when organizations are in the process of working through complex organizational and ownership structures. This can happen when one company acquire another, divests a subsidiary, sets up a joint venture with another company, or must comply with sudden sanctions. In these situations, extra care needs to be taken to balance the need to share information with the need to keep it private.

According to IBM, more than one in three executives surveyed said they have experienced data breaches that can be attributed to merger and acquisition activity during integration. This is because changes as such are one of the most vulnerable times for an organization. When entering a joint venture, merger and acquisition, or divestiture, it is crucial that security requirements are set in place to ensure that only intended users are able to access the files they are attempting to use. Moreover, global operations and workforces tend to share many data stores, which are also vital to protect when changing ownership structures.

When beginning joint venture, merger and acquisition, or divestiture activity, it is important to remember that in assuming assets and liabilities of the target, the acquirer or shared businesses are also absorbing digital platforms, intellectual property, and customer databases. In doing this, organizations can become susceptible to the exposure of cybersecurity threats and compliance risks. Therefore, it is imperative for organizations to realize that even with robust security measures, security dynamics may change vastly during adjustments in the organization's structure. If data stores are not properly secured in these dynamic environments, the vulnerabilities acquired can lead to the demise of an organization.

In the following section, we will be analyzing the challenges joint ventures, mergers and acquisitions, divestitures, and companies facing imposed sanctions encounter when safeguarding data throughout these structural changes.

Challenges

1. Joint ventures

Companies often set up joint ventures with other companies which are legal structures that both companies will contribute assets to, tangible and/or intangible, to address an opportunity better than each company could do independently. A significant challenge with joint ventures, however, is asset sharing. Each company wants to share only the specific assets designated for the joint venture, while not accidentally giving access to assets that need to remain private. Employees assigned to the joint venture may also still have responsibilities to their company outside of the joint venture and require access to assets for both. For example, in a joint venture set up between companies A and B, Company A may share some of their customer data in an internal database with the joint venture. Records of past transactions with those customers, however, may need to be kept confidential, and not be shared with Company B. In this case, policies need to be defined and enforced to prevent anyone who is not an employee of company A from accessing the confidential data. Defined appropriately employees from company B who are contributing to the joint venture will be able to access the data they need to do their jobs without being given access to company A's confidential data.

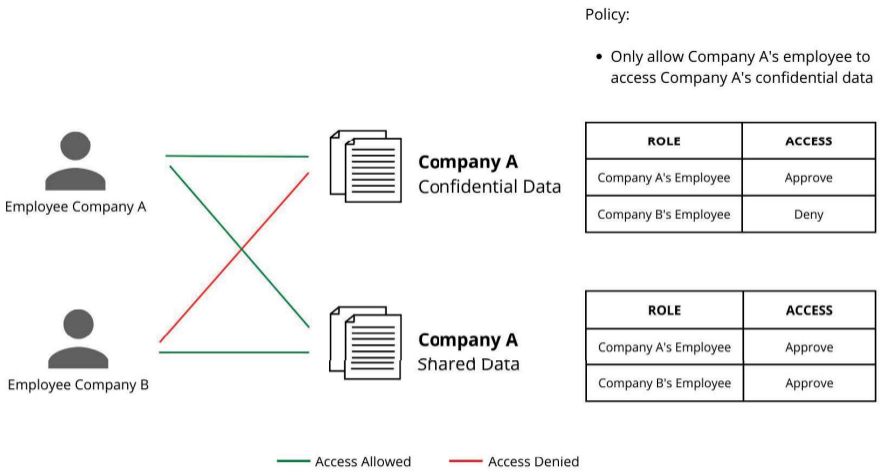

Figure 1: Restricting access in Joint Venture

2. Divestitures

Divestitures offer different challenges for organizations because a single organization needs to be divided into two or more entities, including all employees and other assets. Sometimes, divestitures are created to sell part of a business to another organization, while other times the goal is for the divested unit to operate independently. Regardless, during the process of divestment, care needs to be taken to manage access to systems, assets, and data by members of both the soon-to-be divested unit and the remainder of the organization. When divesting a portion of their organization, access often must be restricted before everything is physically separated. Once the assets, data, and employees that will be part of the newly divested unit have been defined, policies to logically segregate them from the remaining organization need to be defined and implemented. Logical separation in advance of physical separation has separate advantages. The first is that if both the divested unit and the remaining unit are forced to operate separately from each other, it will be easier to identify whether there are ay remaining issues that safeguarding data in joint ventures, divestitures, mergers and Acquisitions need to be addressed before the final separation. The second advantage is that moving all the soon-to-be divested unit's assets to their new systems and locations will be easier if there is already logical separation between the divested unit and the remainder of the organization. Finally, organizations seek to accelerate and reduce cost of the divestiture process via technical service agreement (TSA) without investing heavily to stand up an entire new system landscape for the new company.

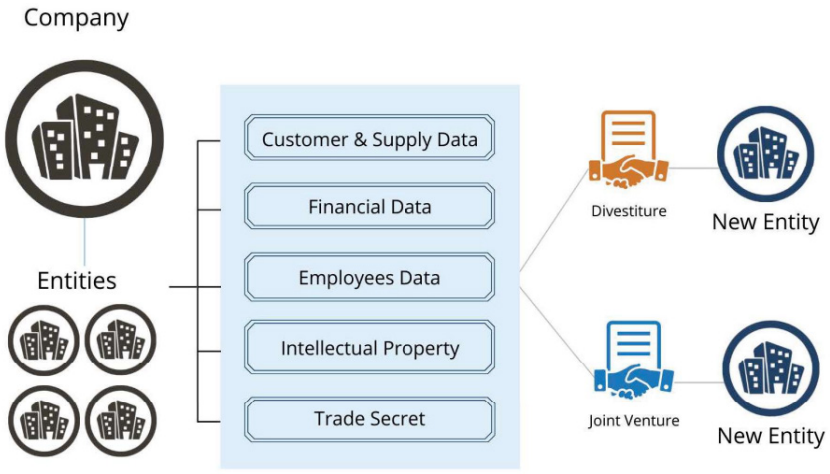

Figure 2: The need to safeguard data moving into Divestitures

3. Mergers & Acquisitions

Divestitures offer different challenges for organizations because a single organization needs to be divided into two or more entities, including all employees and other assets. Sometimes, divestitures are created to sell part of a business to another organization, while other times the goal is for the divested unit to operate independently. Regardless, during the process of divestment, care needs to be taken to manage access to systems, assets, and data by members of both the soon-to-be divested unit and the remainder of the organization. When divesting a portion of their organization, access often must be restricted before everything is physically separated. Once the assets, data, and employees that will be part of the newly divested unit have been defined, policies to logically segregate them from the remaining organization need to be defined and implemented. Logical separation in advance of physical separation has separate advantages. The first is that if both the divested unit and the remaining unit are forced to operate separately from each other it will be easier to identify whether there are any remaining issues that safeguarding data in joint ventures, divestitures, mergers and Acquisitions need to be addressed before the final separation. The second advantage is that moving all the soon-to-be divested unit's assets to their new systems and locations will be easier if there is already logical separation between the divested unit and the remainder of the organization. Finally, organizations seek to accelerate and reduce cost of the divestiture process via technical service agreement (TSA) without investing heavily to stand up an entire new system landscape for the new company.

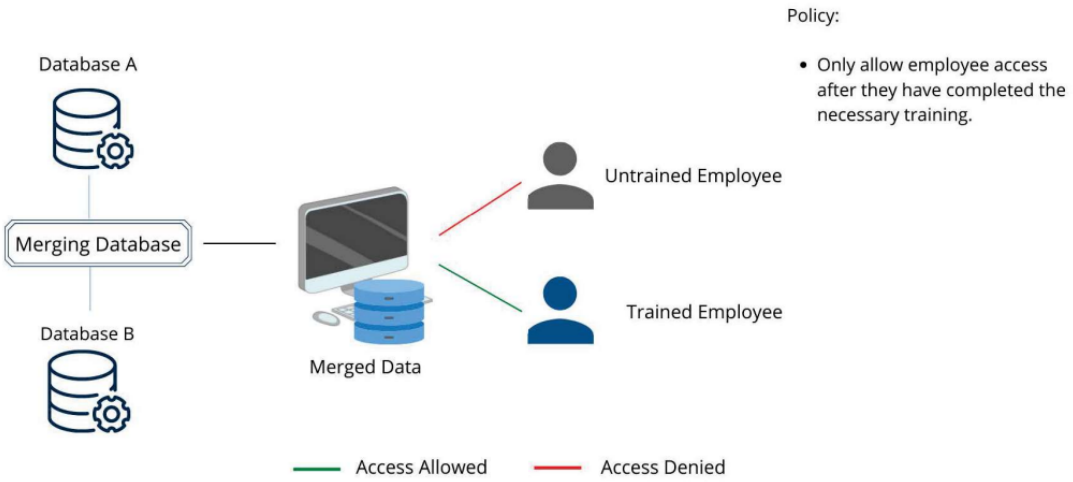

Figure 3: Restricting access in Merger & Acquisitions

4. Sanctions

Sanctions are crucial in the worldwide battle against financial crime, terrorism, and other actions that threaten international peace. These regulations include levying import duties on goods to sanctioned countries, restricting the export of particular goods from a country, and blocking the sanctioned countries' ports. This prevents organizations from conducting business with certain parties or leads to major penalties for those who violate the sanction limitations. In light of sanctions imposed on Russia, which have resulted in corporations pulling out, failed joint ventures and increased process flow, it is more critical than ever for businesses to put an emphasis on effective data governance. Sanction breaches can be caused by a variety of circumstances. According to Deloitte, these variables include absence of a data governance program, sanctions screening software of filter flaws, as well as insufficient customer due diligence. Sanctions often result in the need to carve out certain business operations and segregate data related to the sanctions. Additionally, it is critical that unauthorized transactions and operations related to sanctioned parties be blocked. Hence, there is a need for an operational company-wide data governance initiative to ensure workforce productivity while keeping data safe. An effective data governance program can segregate data, controlling access to business-critical data of the sanctioned parties, and helps prevent any transmission and sharing of sensitive data with parties related to sanctions.

Figure 4: Importance of segregating data during Sanctions

Key requirements to Safeguard Data

Although safeguarding data in these dynamic environments can be quite complex, there are several aspects that can improve your business' cybersecurity and compliance practices during these organizational changes. To prevent data breaches during these organizational structure changes, it is vital to automate policies and procedures to restrict access to sensitive information dynamically and protect data with dynamic data masking and data segregation technique. It is essential for data owner and business user to be able to write policies with a business-friendly GUI without coding. This will allow for data to be protected continuously as policies can be managed directly by the business stakeholder, as there is no inherent need for a developer to code policies. With this, it ensures that the policies are current and effective in preventing unauthorized access. Additionally, proper policy governance is crucial as it ensue es integrity, approval, and proper lifecycle management of policies; coupled with delegated administration, segregation of duties, and regular monitoring and auditing of policy activities.

How to safeguard Data

Based on the previously seen challenges in major organizational structure changes, it can be observed that these shifts can require the need to change drastically in the area of access control, data sharing, data flow, and merging of systems. The following section will illustrate the four key pillars on how to address the key requirements to safeguard data, regardless of the type of organizational change.

Policy Development

In each of the scenarios discussed above, the environment is evolving, with organizations, employees, and assets that need to be shared yet protected. Within such a dynamic environment, the policies that protect data must also be dynamic. Policy development, while sometimes overlooked, plays a major role in safeguarding data in dynamic environments. Having a business-friendly digital policy management system that allows for easy and simple policy development allows for policies to remain up-to-date and ensure sensitive information remains secure. Using a 4GL policy language with a point and click GUI, non-technical users can express and manage information policies easily. Since 4GL is a non-procedural language that utilizes a natural language syntax similar to English, it eliminates the complexities associated with other authoring policy languages such as 3GL, which requires programming knowledge. 4GL policies are simple to learn, understand, write, and maintain, as they require no coding. Meaning business- oriented power users can create and maintain policies on their own, without the need of a technology expert.

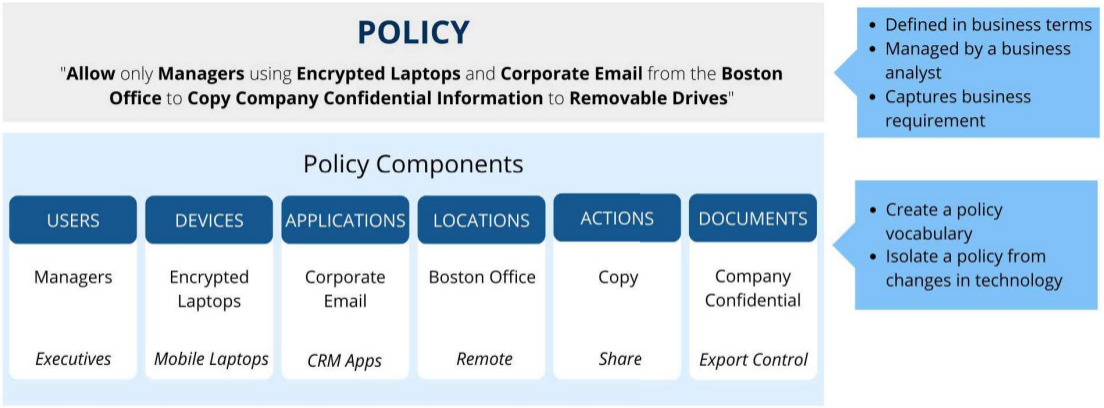

Figure 5: Policy writing using 4GL

Additionally, using dynamic authorization with ABAC will work to significantly streamline management processes, making it easy for power users to manage access control. With a few simple policy changes, hundreds of roles can be changed. This removes the need to individually administer thousands, or even hundreds of thousands of access control lists and other role assignments. Because of this, it also eliminates the need to deploy expensive and complex identity governance solutions. This is extremely beneficial in major organizational structure changes, but also day-to-day changes in dynamic work environments.

Policy Management & Governance

Policy governance plays a vital role in ensuring integrity of the policy and policy management process. Proper policy governance is essential to assure data is safeguarded continuously. An easy to use policy management facility will simplify administrators' ability to ensure proper policy governance, through selecting how users can be limited to certain actions, and providing a system of 'checks and balances' throughout the policy lifecycle. With this, it ensures proper lifecycle management of policies, delegated administration, segregation of duties through ABAC, and audits. All of these aspects warrant only authorized users can modify and create policies, ensuring teams experiencing changes to their organization's structure, can only access files they are intended to view. With policy lifecycle management, power administrators are able to ensure that certain users can update, modify, and delete policies as needed, ensuring that the proper level of access is granted to individuals throughout the entire lifecycle of the policy. Delegated administration further aids in policy governance, as it allows power administrators to specify a subset of individuals, such as policy analysts, security administrators, or auditors, to be able to enact changes to policies as deemed appropriate to their role.

For example, a power administrator can assign a policy analyst to be able to create and edit policies, but not deploy policies. Whereas a security administrator can deploy policies but cannot create or edit policies. While a policy auditor, may be able to view policies but is not able to make any changes. Through this, it also demonstrates a clear segregation of duties throughout the policy development lifecycle and helps enforce internal controls. Many industry and government regulations require strict enforcement of boundaries, as such, to preserve confidentiality when handling sensitive data. This is also true, in dynamic environments that are facing imposed sanctions, along with joint ventures, mergers and acquisitions, and divestitures.

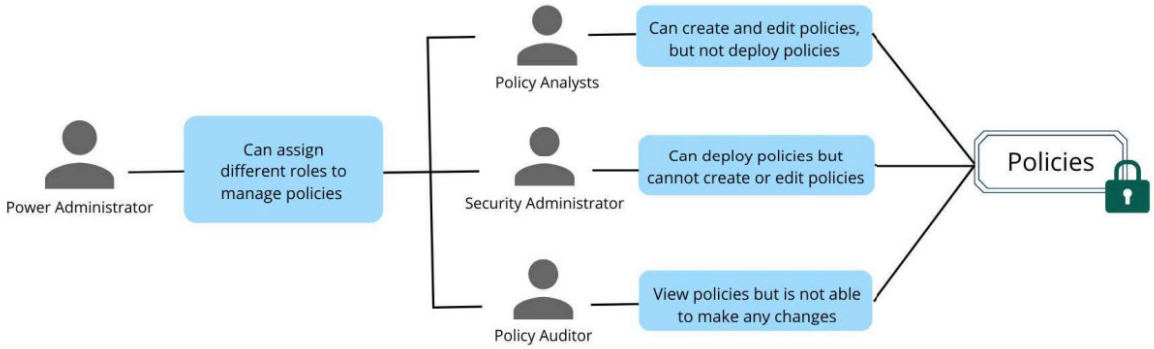

Figure 6: Importance of delegated administration in regard to policy creation

Policy enforcement

By defining policies based on the attributes of the user's accessing data, or based on attributes of the data itself, policies using attribute-based access control (ABAC) and dynamic authorization can be enforced at runtime by evaluating attributes during data access attempt. In doing this, ABAC can determine which applications, types of data, transactions users can submit, and the operations they can perform, automatically based on contextual factors. With this, organizations using ABAC can make concise decisions based on real-time information.

Through the use of policies containing dynamic field-level data masking and record-level data segregation conditions and logics, organizations are able to automate the protection of data seamlessly within the user workflow and business process. With dynamic data masking, the original data is hidden with modified content to protect the sensitive information. This ensures that users can only see the fields on the record to which they have been granted access to. Those who do not have the necessary permissions will find the value of the field to be masked based on the pattern defined in the policy. Data segregation dynamically filters information based on policy, shielding data from unauthorized users until access is granted. Authorization can be determined by environmental attributes, such as industry, location, department, project assignment, or any other attribute of the user.

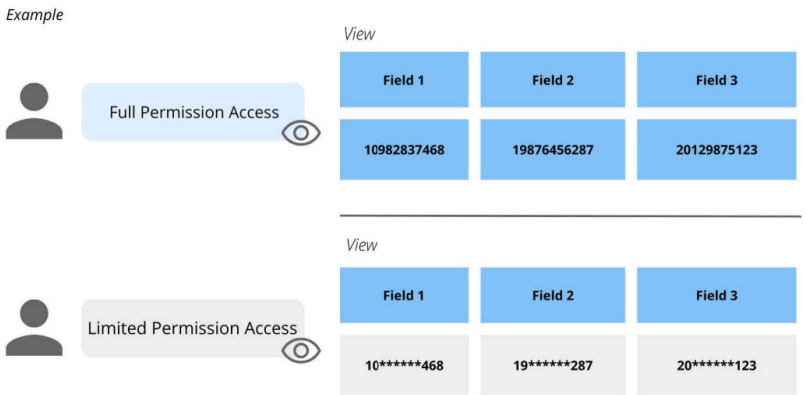

Figure 7: Partial- masking data for unauthorized users

Preventing unauthorized access to sensitive data through fine-grained authorization helps protect data and address compliance requirements all at once. Fine-trained authorization can work to avert users from attempting to bypass and insert, modify, or delete any information, while policies can allow used s to view a data set, without being allowed to manipulate any of the fields present. Additionally, privileged users such as power users— commonly administrators or developers, can be permitted to change permissions, insert or delete tables, export and back up records, along with other actions necessary to be performed by the power user's role will aid in safeguarding data. These permissions can be restricted so they are not abused. For example, a power user may be able to delete tables, but not all— they can delete all tables except two, as explicitly stated in the policy.

Auditing & Monitoring

Auditing and Monitoring are essential controls for detecting, preventing, and deterring irregularities in an organization. The intent is to incorporate a system of external reviews to assist in the identification of areas that require improvement while simultaneously ensuring the existing systems are free from error.

In enterprises that are experiencing organizational structure changes, it is vital that the audit and monitoring process is streamlined and automated. Moreover, auditing and monitoring are some of the most critical elements of regulatory compliance because they evaluate whether internal controls are adequate and productive. By keeping all the data in one central location, auditing makes it easy to identify high-risk areas. As a result, organizations can run risk assessments, find gaps in compliance, and address potential risks before they get out of hand.

Various data privacy regulations require organizations to audit the use and distribution of non-public material information. This includes having knowledge of where the information is, who has access to it, and what they can do with it. Trying to keep track of all of this manually is expensive, time consuming, and error prone, which can cause enterprises to be out of compliance. Automating audits will simplify this process and provide error-free reports. Moreover, being able to monitor and provide insights into information usage is very important in global enterprises and for organizations that previously operated in sanctioned regions. It is also vital to be able to track access requests, whether allowed or blocked. This will help simplify compliance management audits, which are crucial in large organizational structures. Additionally, analytics of user behavior and access patterns can also be very helpful since it allows audit administrators to better understand the use of information, along with the level of associated risk. Through monitoring and auditing access usage, organizations can maintain high security vigilance, a critical aspect for companies who are facing organizational structure changes as this is when they tend to experience increased cybersecurity threats due to media exposure.

Example

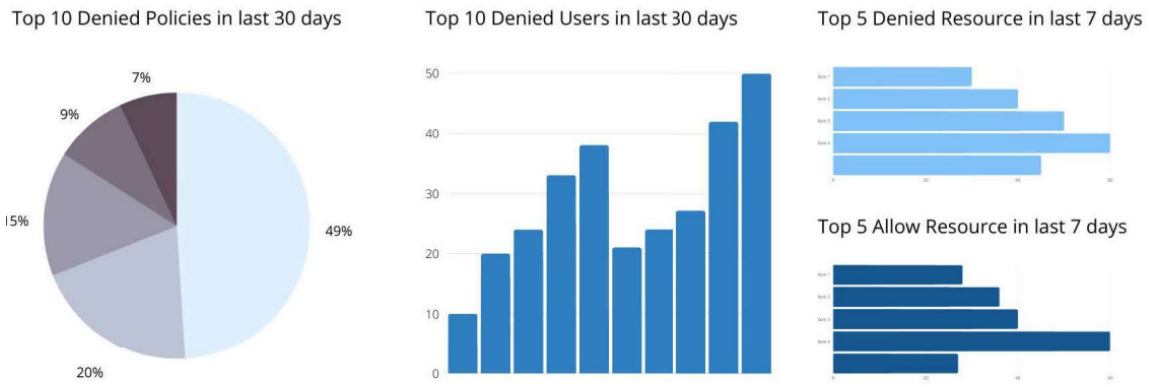

Figure 8: Example reports on policy enforcement

Nextlabs Solution

To address the needs of enterprises facing major organizational structure changes as those previously described, NextLabs has designed its Data Access Security and Entitlement Management families of products to allow organizations to control access and protect data through flexible policies that are dynamically enforced at runtime in the application and data access laver. NextLabs uses its Active Control Policy Language (AC PL), a fourth-generation policy language (4GL), which is based on the NIST Attribute-based Access Control framework (NIST SP 800-162) and the OASIS XACM L standard for access control. This is the underlying language for NextLabs' solutions that allows users to express and manage information policies. This "no-code" policy language enables business users to be able to update policies as needed, ensuring that policies will always remain up to date as there is no need for a technical user to code policies. Since NextLabs' solutions contain dynamic authorization and ABAC, it also streamlines management processes, allowing access requirements created by the major organizational changes to be addressed quickly and easily.

NextLabs' solutions also provide the ability to ensure proper policy governance, allowing administrators to only perform specified permitted actions when creating policies. This along with the approval workflow and segregation of duties ensures that the proper level of access is granted to individuals throughout the lifecycle of the policy. The enforcement at the application and data access laver ensures that policies are enforced regardless of how the data is being accessed. NextLabs helps enterprises overcome challenges of safeguarding data and restricting access to sensitive information, through fine-grained data-level security controls, protecting data and addressing compliance requirements all at once. Additionally, NextLabs' solutions can dynamically segregate and mask data, protecting data at the record and field level ensuring that only intended users can access data. Through dynamic security controls and access restrictions, it allows organizations to ensure that their sensitive information remains protected during, before, and after any structural changes.

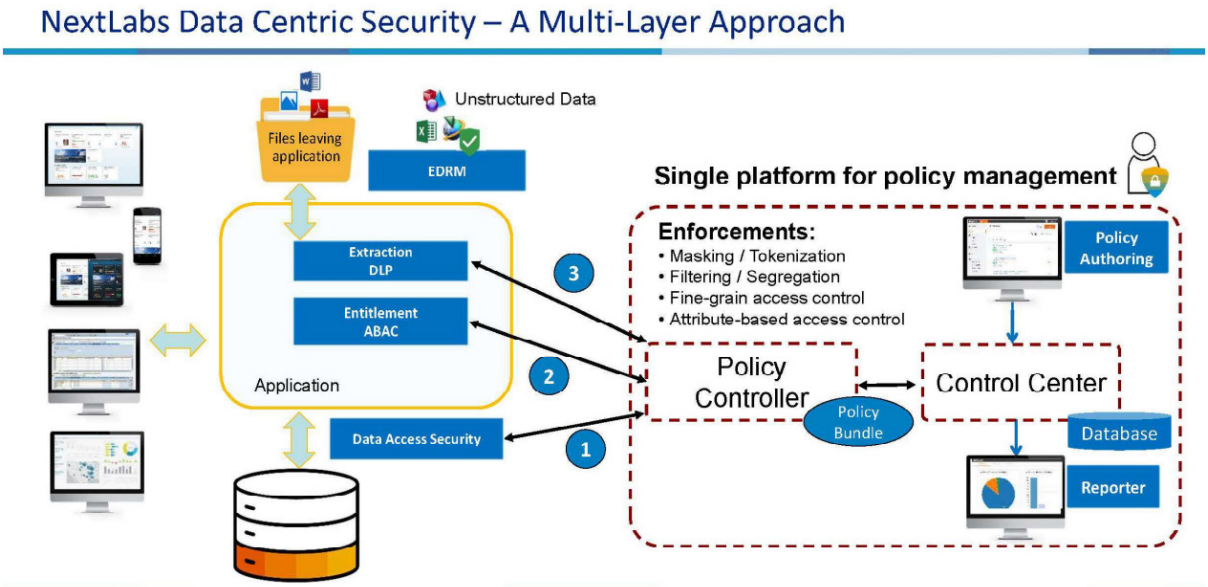

Figure 9: NextLabs' Data-centric approach to safeguarding data

NextLabs' solutions also track, report, and alert on risky access activity through its centralized dashboards and reporting facility. This helps to ensure high security vigilance, while also allowing administrators to understand user patterns and analytics. With automated auditing, it simplifies the audit process, ensuring the organization remains in compliance with regulations. Through the implementation of NextLabs' Data Access Security and Entitlement Management, organizations can meet the key requirements as outlined above to safeguard data in dynamic environments.

Conclusion

As seen in this white paper, organizations facing sanctions, entering joint ventures, mergers and acquisitions, or divestitures, experience a series of challenges when it comes to safeguarding their data. In order to overcome these challenges and avoid risks commonly seen in these organizational changes, it is crucial that enterprises follow the four pillars and keep tight controls in place, that way there is no relaxation of security protocols during integration or other changes. NextLabs' solutions work to safeguard sensitive data through the four pillars discussed, policy enforcement, governance, development, and auditing and monitoring. These pillars outline how organizations can easily ensure their data remains secure in a globally competitive and dynamic environment with an evolving distributed and virtual workforce. While this white paper only covered some of the situations encountered in major organizational structure changes, it is vital to safeguard data during all organizational adjustments as that is when enterprises are most vulnerable.

For more information, watch NextLabs' webinar on Segregating Data in Joint Ventures and Divestitures.

References

Deloitte. "Data Management: Why It Matters for Effective Sanctions Screening." Deloitte Switzerland, 2022. https://www2.deloitte.com/ch/en/pages/forensics/articles/data-management-sanctions-screening.html.

Deloitte. "In a Divestiture, Proactively Address Comingled Data." The Wall Street Journal, January 21, 2022. https://deloitte.wsj.com/articles/in-a-divestiture-proactively-address-comingled-data-01642790433.

Deloitte. "Sanctions and Their Relevance for Non-FS Organisations." Deloitte Switzerland, 2022. https://www2.deloitte.com/ch/en/pages/forensics/articles/sanctions-and-their-relevance-for-non-fs-organisations.html

Harroch, Richard. "Data Privacy and Cybersecurity Issues in Mergers and Acquisitions." Forbes, November 11, 2018. https://www.forbes.com/sites/allbusiness/2018/11/11/data-privacy-cybersecurity-mergers-and-acquisitions/?sh=5c97a52c72ba

IBM Corporation. "IBM Report: Cost of a Data Breach Hits Record High during Pandemic." IBM Newsroom, July 28, 2021. https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

Kessler, Sarah. "The Week in Business: Economic Sanctions Take a Toll."The New York Times, March 13, 2022, sec. Business. https://www.nytimes.com/2022/03/13/business/the-week-in-business-economic-sanctions-russia-ukraine.html.

Rapoza, Kenneth."Worst-Ever Russia Sanctions Set to Become a Business, Market Nightmare." Forbes, February 28, 2022. https://www.forbes.com/sites/kenrapoza/2022/02/28/worst-ever-russia-sanctions-set-to-become-a-business-market-nightmare/?sh=27288b2d4edb

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.