The Eight Most Common Data Security Challenges that DSPM Solves

SYMMETRY SYSTEMS

Contents

Highlights from The Eight Most Common Data Security Challenges that DSPM Solves

To put it simply, organizations depend on data to operate. From day-to-day operations to strategic decisions, data keeps an organization ticking. The volume of data is immense, and data growth is explosive. And with all that scale and explosive growth comes data security challenges. As the pioneer behind Data Security Posture Management (DSPM), Symmetry System's DataGuard is redefining what a data-centric approach to cybersecurity looks like–security from the data out, not the perimeter in–using a deployment approach that can examine data in different environments: the cloud, on-prem, or both.

Using information gleaned from millions of customer data points, this document presents the eight most common data security challenges that Symmetry regularly sees. We discuss how eight issues happen, the risks associated with them, and the remediations and best practices to improve overall data security. Highlights include:

Data Security Posture Management

DSPM directly addresses the issues security, data, and IT teams have related to understanding the details associated with sensitive data–who has access, how it is being used, where it's located, and how safe it is. DSPM is about data visibility–first by identifying data at the data object level, mapping which identities that have access to what data, and then exploring how the data flows across the environments.

To learn more about DSPM, go directly to page 7.

The Zero Trust Component

Comprehensive DSPM solutions like DataGuard accelerate Zero Trust adoption by providing SecOps, InfoSec, IT, and data teams accurate insight into who has access to data and from where, organizations can identify data security risks, as well as actionable recommendations on how to reduce that risk.

Curious about how Zero Trust fits into DSPM, go to page 9.

In This Case, Eight Is Not That Great.

Let’s discuss these eight challenges of data security:

1 Lack of Data Inventory

Organizations simply don’t know what data they have, where it is, or why it is important. You can uncover more about data inventory on page page 11.

2 Dormant Data Stores

They’re old, unused, and potentially ripe for an attack because no one’s paying attention. Read about dormant data stores on page 13.

3 Over-Privileged Data Stores

Just like over-privileged identities, an over-privileged data store has widespread access enabled, inviting trouble. Read more on page 15.

4 Dormant Identities

The single most common data security issue and one of the overlooked paths to breaches and attacks. Learn more on page 17.

5 Over-Privileged Identities

It’s common for organizations to overestimate the level of access and privilege an identity needs. More information on page 20.

6 Delayed or Incomplete Employee and Vendor Offboarding

Symmetry’s engineers have discovered instances where departed vendors or employees still retain admin-level access to sensitive systems and data. We think you can pretty much guess the risks. Check out page 22.

7 Inadequate Segregation of Duties between Development, Test and Production Environments

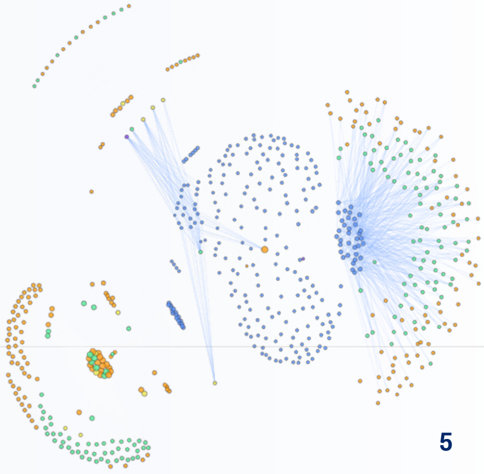
Companies often fail to enforce segregation of duties between development, test, and production environments. You can find out more on page page 25.

8 Application and Backup Misconfiguration

There are a lot of ways applications, systems, or backups can be misconfigured. Symmetry often sees things like inadequate access controls, unprotected files and directories, and access to unnecessary or unused features. Find out the implications of application and backup misconfigurations on page 27.

How DSPM and DataGuard Work

Understand how DSPM works and how it can offer full visibility into data stores, including the location of sensitive data, who has access to it, and what operations have been performed against it. Read about the data collection, analysis, and reporting steps on page 27.



From the CEO

The cybersecurity industry has been approaching the “cybersecurity problem” from the wrong perspective for many years. We have been conditioned to secure the perimeter, then endpoints, and, lastly, users from threats and attacks. Threat actors don’t care about your perimeter, users, or endpoints. When planning an attack, it’s all the same to them; a means to an end, a door into your systems, and a way to achieve their ultimate goal, which is attaining your data. To properly secure organizations from cyberthreats, I believe we, as an industry, need to build security programs from the data out. This means starting with the data, identifying who has access to the data, and then layering on additional endpoint and perimeter protection. We built DataGuard for this sole purpose–to secure data from the data out. Our Zero Trust Data Assessments highlight why this approach is sorely needed.

Over the past year, our data security team has worked closely with over a dozen customers to assess their data security posture. The team installed and configured DataGuard, our Data Security Posture Management (DSPM) solution, in Microsoft Azure, Google Public Cloud, and Amazon Web Services environments. We let DataGuard do what it does best, enumerate all our customer’s data at the data object level, map out which identities that have access to what data, and examine how the data flows across the environments. From there, DataGuard presents visual evidence of risks to the environment, which we show to our customers in our Zero Trust Data Assessments.

Our Data Assessments are designed to provide our customers with a deep review of each of their data security postures, with highlights of their data security risks, followed by prioritized actionable recommendations on how to quantitatively reduce these risks. After reading all the individual Assessments, I wanted to share with you the most common data security findings we uncovered over the past year. My hope is that you can use what we’ve learned from these Assessments to start building out both an understanding of your modern data security challenges and a data-first security strategy.

If you have any questions about this digest, or would like to see how DataGuard collects the information described here, please do not hesitate to reach out to me or my team.

Sincerely,

Mohit Tiwari
CEO, Symmetry Systems

What Is Data Security Posture Management(DSPM)?

Data Security Posture Management (DSPM) was defined by Gartner® in their Hype Cycle for Data Security, 2022 as a product that "provides visibility as to where sensitive data is, who has access to that data, how it has been used and what the security posture of the data store or application is. This requires a data flow analysis to determine the data sensitivity. DSPM forms the basis of a data risk assessment (DRA) to evaluate the implementation of data security governance (DSG) policies."

In the 2022 Gartner® Cool Vendors™ in Data Security – Secure and Accelerate Advanced Use Cases published on 19 April, 2022 Symmetry Systems was named a Cool Vendor.

At its core, the best and most comprehensive DSPM solution focuses on securing an organization from the data out, using a deployment approach that can examine data in the cloud, on-prem, or both.

A Data Security Posture Management solution will also answer four key and critical questions for a customer:

- **Where is my sensitive data?**
- **Who has access to it?**
- **How has it been used?**
- **What is the security posture of our data store?**

Finally, a DSPM solution will also offer meaningful guidance to the customer on how to constantly improve their data security posture–and more importantly, automate the process so the burden to remediate an issue isn't on already under-staffed data, security, or IT teams.

> Symmetry Systems' DSPM solution–DataGuard–was the first platform to be described by Gartner as a "Data Security Posture Management" (DSPM) product.

What is DataGuard?

Symmetry Systems DataGuard is a Data Security Posture Management (DSPM) solution that embeds the Zero Trust philosophy in securing data in hybrid-cloud data stores. Modern security teams use DataGuard to help businesses develop a complete understanding of what data types and data stores they have, where the data is stored, who and what is entitled to it, how it is secured, and in what manner it has been accessed. The unique combination of data classification, data operations, and identity information provide insights that every organization needs to secure their data.

DataGuard enables businesses with precise and accurate insight into their data security posture and associated data risks across AWS, GCP, Azure, and on-premises environments, including but not limited to most data store types, like RDS, PostgreSQL, or MongoDB–without having data ever leave the customer's environment.

The cybersecurity industry is saturated with security solutions that focus on building defense in depth beginning at the perimeter and working toward the data. DataGuard builds security from the data out, directly addressing data objects and examining the intersection of identity, data stores, and data flow to answer important questions like:

- **Where is our sensitive data?**
- **Who has access to it?**
- **What operations have been performed against it?**

With DataGuard, your cross-functional teams, such as security operations, cloud security, compliance, and identity & access management, can enforce least privilege, sustain regulatory compliance, improve their data security posture, and outpace ever-growing data security risks and threats.

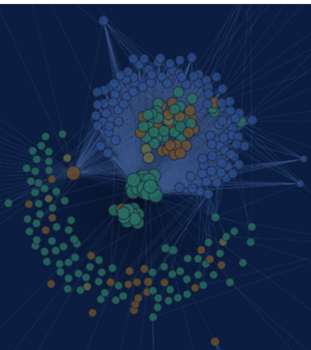
The cybersecurity industry is saturated with security solutions that focus on building defense in depth beginning at the perimeter and working toward the data.

What Is a Zero Trust Data Assessment?

Our customers deploy DataGuard, our DSPM solution, in their cloud and on-premise environments within minutes. During a time-limited engagement, Symmetry Systems data security experts use DataGuard to conduct a deep investigation into each customer's data security posture and then develop a Zero Trust Data Assessment that showcases their data security risks and provides actionable recommendations on how to reduce that risk.

Armed with DataGuard, the Symmetry Systems data security team performs an agentless scan and quickly identifies your hybrid cloud data stores to unearth challenges, misconfigurations, and violations at scale. With evidence documented in the Zero Trust Data Assessment, you can proactively adjust identity access management (IAM) policies on individual data objects, users and roles. This way they can ensure that only the appropriate users and technologies have access to only the appropriate data, and that scoped permissions for those users are in line with Zero Trust and least privilege requirements.

Zero Trust Data Assessments arm our customers with clear and immediate insights into data access, user permissions, and operations taken against data. Our customers' security teams use Zero Trust Data Assessment findings and recommendations to reduce data access entitlements that otherwise might have been too permissive, reducing the risk of data breaches and other unintended data access.



Zero Trust Data Assessments provide:

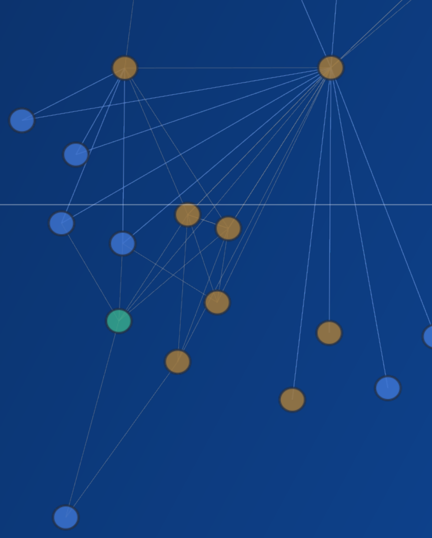
A complete data inventory of a customer's hybrid cloud data.

Immediate visual insights and evidence of Zero Trust violations and data security risks across their hybrid cloud data stores.

Detailed evidence that can be used to answer critical data security posture questions that help outline a successful Zero Trust-based or data-first security strategy.

Recommended actions to fortify customers' data security posture to ensure the Zero Trust philosophy can be applied across the organizations' data stores.

The Eight Most Common Data Security Challenges



1. Lack of Data Inventory

What Is a Data Inventory?

Data inventory refers to the process and output of identifying and categorizing all of the data within an organization. This includes providing searchable insight about where the data is stored, how it is used, who has access to it, and the level of sensitivity and importance of each piece of information. A robust data inventory is a critical component of any effective data-centric security strategy, enabling organizations to proactively identify and address potential security threats before they become a data breach.

Why Don't Organizations Have a Data Inventory?

It's hard. No organization has a single cloud anymore, let alone a single data store. The scale and complexity is mind boggling, when you realize that organizations have millions of data objects across thousands of data stores. This explosion in data everywhere is an unintended consequence of the relative inexpensiveness of data storage. Organizations can and do freely store everything in the hope that it can become useful in the future. They then store it for long periods, because they might need to for regulatory compliance reasons.

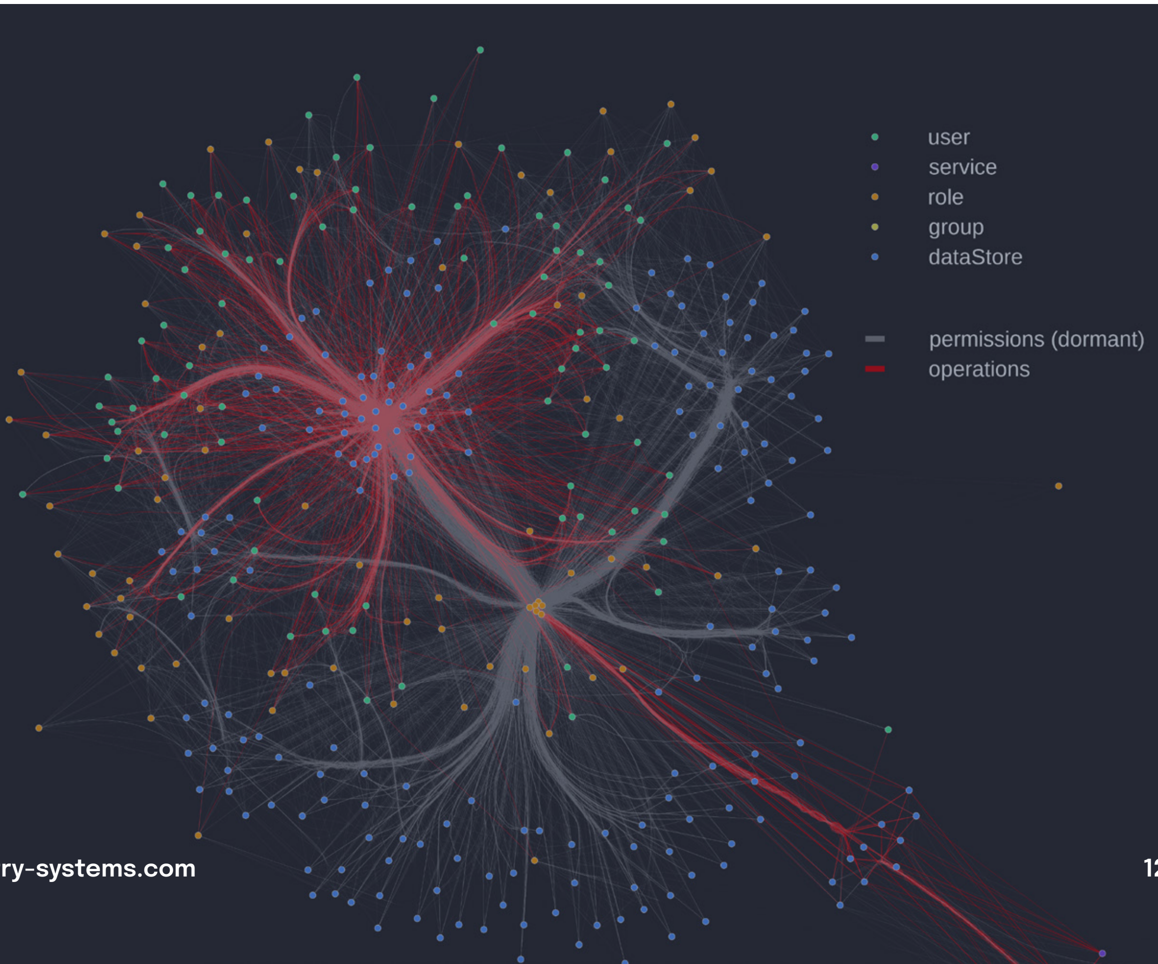
But hidden in this data (that is often collected somewhat haphazardly) is typically a large amount of sensitive information. Identifying the sensitive data at scale and without breaking the piggy bank is challenging. While some sensitive information is obviously easy to detect across organizations based on the content (i.e. credit card numbers, dates of birth, Social Security Numbers, etc.), it is prone to a high false positive rate. However, most sensitive data is organizationally specific, based on both its context and content. For example, the content of a data store containing a list of food isn't immediately identifiable as sensitive, but with context linking this to a patient's food allergies, the sensitivity increases dramatically.

Lack of Data Inventory: The Risks

Without knowing what data they have and where it is, organizations are unaware of the magnitude of risk they are exposed to, such as penalties and legal liability from non-compliance or operational impact on organizations from unauthorized access, destruction, or alteration of data, as described in our recent blog on the four horsemen of data security.

Best Practices for Developing a Data Inventory

The lack of a data inventory is an easy challenge to start addressing and is the first step in any Zero Trust Data Assessment. Our agentless discovery approach enumerates all cloud data stores to quickly identify the data owners and all resources that might contain sensitive data. Generally speaking, if it's in the cloud, we have a connector to scan data from any data stores. We then use our built-in data classifiers to identify sensitive information. Our sampling approach is customizable and allows organizations to quickly identify data stores that contain sensitive data and improve their security posture. Our team of data scientists will further help train custom classifiers and reduce false positives in your environment, providing an accurate and custom view of your data inventory.



2. Dormant Data Stores

What Are Dormant Data Stores?

Dormant data stores are those that have not been accessed or contain data that has not been used in an extended period of time. (Typically any data store with 90 days or more of inactivity is considered dormant.)

How Do Dormant Data Stores Happen?

Organizations continually collect significant volumes of customer information and other data, and store it for long periods. This may be due to regulatory compliance reasons, but more commonly it is done in the hope that it can become useful in the future. Just because the data store is dormant, does not mean that the data isn't required, useful, or valuable; but it certainly increases the data security risk. Our engineers and scientists have found that the majority of organizations that have dormant data stores are either not aware of or are unsure if the data in the data store is sensitive and protected by privacy and compliance regulations.

Dormant Data Stores: The Risks

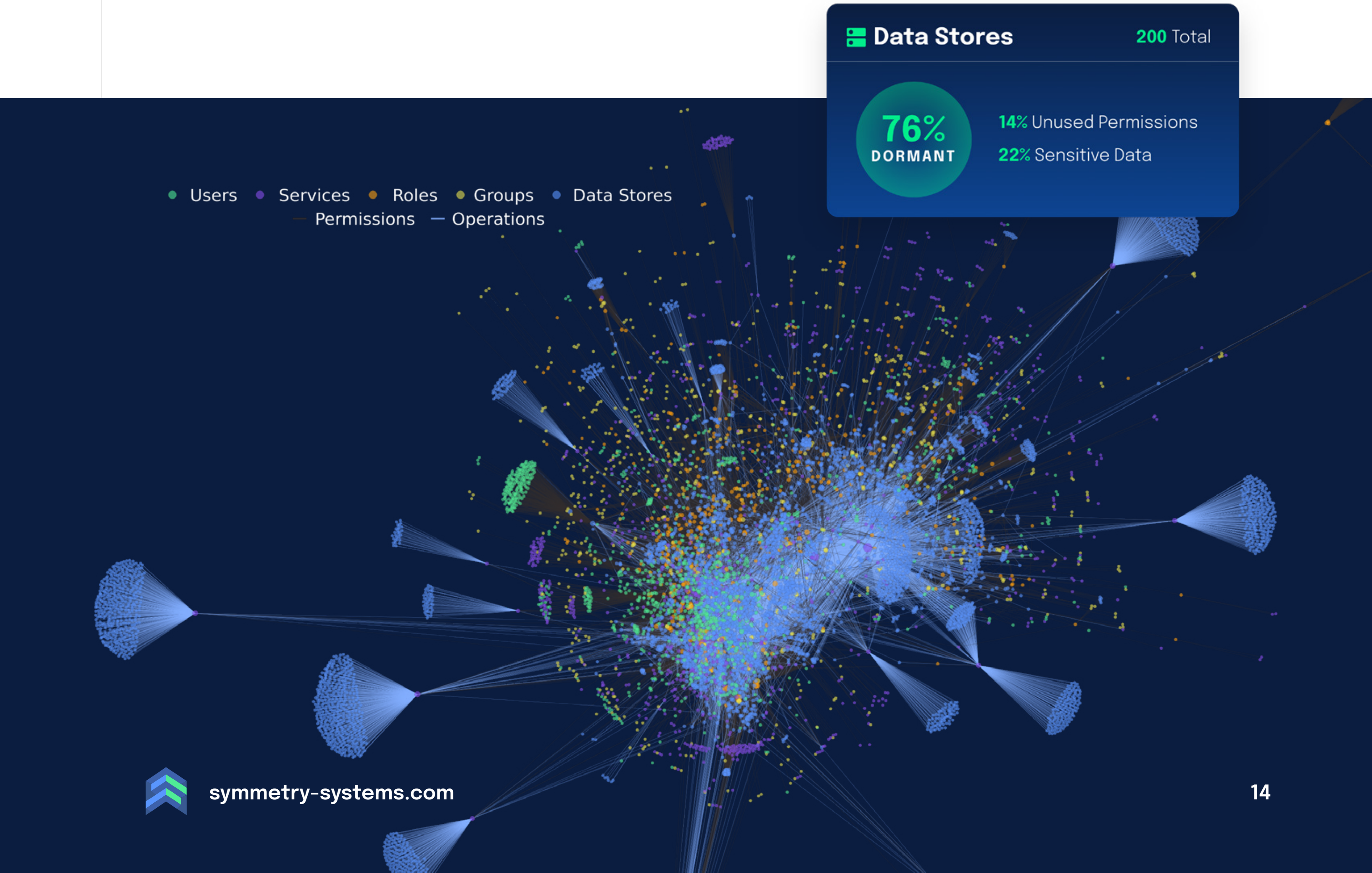
Leaving data stores dormant or otherwise unchecked unnecessarily widens the attack surface and the blast radius of a data breach. This is because even if the data stores are not being accessed or utilized on an ongoing basis, they may still be accessible by a malicious third party, employee, or threat actor who can capture or manipulate the data for malicious purposes.

Simply put, dormant data stores keep doors open for attackers. In many cases, knowing data store specific names, as leaked on the dark web, allows attackers to try credentials and validate their functionality.

Remediations and Best Practices for Dormant Data Stores

The lack of awareness of dormant data stores and the data they house are a relatively easy challenge to address to quickly reduce the attack surface and data blast radius. Generally speaking, if a data store is deemed dormant, organizations should consider offboarding the data store to secure cold storage or archive it in other ways to minimize the attack surface. Moving a data store to cold storage can help the organization reduce the financial burden of cloud data storage. It can also provide an opportunity to reduce access to it.

As part of our Zero Trust Data Assessments, Symmetry Systems recommends that its customers immediately evaluate dormant data store permissions. In addition, our DataGuard solution can identify and classify protected data in the data store (such as Privately Identifiable Information) or mission critical data (as defined by the customer), as well as the customer's or data store's risk posture. With this information, we recommend that organizations build a policy for dormant data stores that outline when permissions to data stores should be offboarded and whether data stores should be moved to cold storage, deleted, or backed up. This policy should be informed based on the value of the data to the organization, the identities that have access to the data, and the overall attack surface.



3. Over-Privileged Data Stores

What Are Over-Privileged Data Stores?

An over-privileged data store is one that has widespread access enabled to allow operations on data by identities that typically would not need it. It can be a data store that multiple individuals in a department have access to or one in which permissions have been set at the data-store level rather than the identity level, but only a limited number of individuals have a clear business need to access all data in the data store.

How Do Over-Privileged Data Stores Happen?

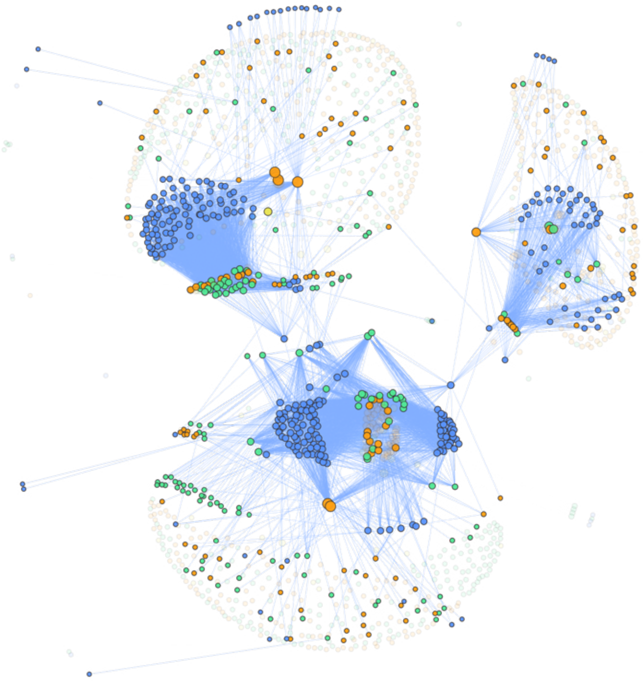
Virtually every organization for which Symmetry System developed a Zero Trust Data Assessment had data stores that were deemed overprivileged. In general, project managers or project owners often hand out credentials without necessarily understanding the direct or derived permissions of those credentials. In addition, managers and project owners may not have total visibility into what kind of access or functionality the permission can grant. On top of this, permission management is also different for each platform. This raises the question of who at the organization should be the ultimate authority for setting permissions for identities, be they employees, systems, technologies, or applications.

Over-Privileged Data Stores: The Risks

The interesting challenge that engineers and scientists at Symmetry Systems continue to uncover is the disconnect between organizational teams that have responsibility for managing permissions to data. Security teams tend to try to manage permissions for identities, while development, data, and engineering teams often manage permissions of the data stores and related technologies. When permissions are managed in silos like this, conflicting permissions tend to favor the more permissive approach, nullifying any security best practices and attempts at least privilege. This puts the organization at a higher risk of data breaches, leaks, and misuse. The ability to manipulate, delete, or move data must be assessed at the individual identity level, to ensure granular control over the data and to ensure the data blast radius of a compromised identity is held in check closely.

Remediations and Best Practices for Over-Privileged Data Stores

Organizations are going to have different methodologies to choose from to set up permission management. These methodologies may be identity or role driven, so best practices may be a little different for each organization. A common best practice across organizations is the manageability of the chosen methodology. When distributing permissions, organizations need to make sure all parties clearly define ownership and accountability. Further, any relevant practice area–security, engineering, development, data, IT, and even the project management team–needs to have full knowledge of what those permissions can do and how they operate. Finally, there must be constant review and clean up of permissions as part of standard business operations.



● Users
● Services
● Roles
● Groups
● Data Stores
— Permissions
— Operations

4. Dormant Identities

What Is a Dormant Identity?

Dormant identities are identities that have been inactive for a long period of time. They can include users, roles, groups, service accounts, or even devices. Dormant identities accumulate in every environment due to failure by organizations to to clean up these inactive users. If left undeleted, cyber threat actors can take advantage of dormant identities. If a threat actor commandeers a dormant identity, it is unlikely that the security team will notice the identity's use, since the original user is not actively using the identity.

How Do Dormant Identities Happen?

The most common data security challenge that Symmetry System regularly observes is a proliferation of dormant identities. Dormant identities happen, because, in order to conduct business, organizations tend to quickly grant employees, vendors, contractors and other third-parties access to systems, databases, applications, and other technologies.

Granting access to applications is easy, however, keeping track of who actually needs access to which systems and who actually continuously uses those systems is a bit tricky. Symmetry Systems has found that organizations tend to err on the side of granting broad access to users on the off chance that those users might eventually need to access certain systems. In addition, some organizations do not have well defined processes in place to review identities on an ongoing basis and to remove dormant identities when necessary.

Dormant Identities Contribute Significantly to Compromised and Stolen Credentials and Data Breaches

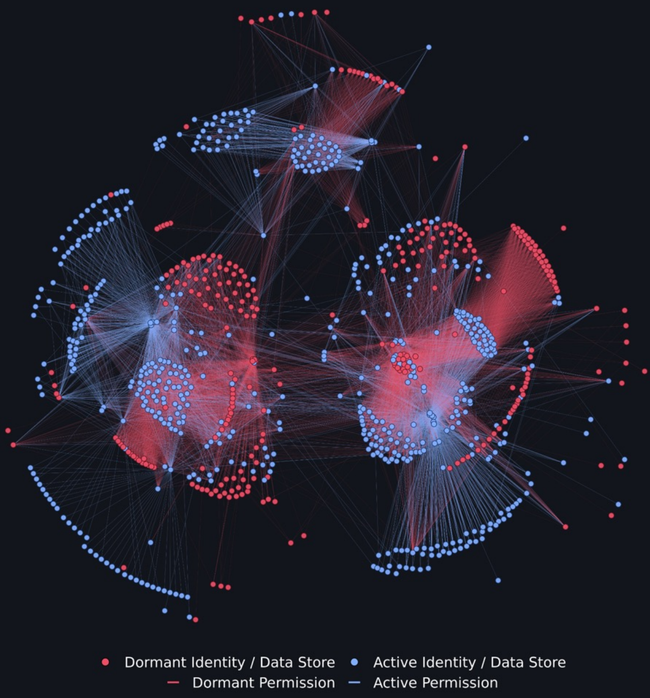
According to the 2022 Verizon Data Breach Investigations Report (DBIR):

- There has been a 30% increase in stolen credentials since 2017.
- 80% of breaches in web application attacks can be attributed to stolen credentials.

According to the 2022 IBM Cost of a Data Breach Study:

- Stolen or compromised credentials were the initial attack vector with the longest mean time to identify and contain the breach, at 327 days.
- Breaches caused by stolen or compromised credentials had an average cost of USD 4.50 million.

Organizations don't have visibility into their data stores, which means they don't fully understand who has access to what data, how that data is being used, or if dormant identities have been cleaned up.



Dormant Identities: The Risks

Threat actors seek out the path of least resistance to obtain sensitive information, and dormant identities are the quickest way to the goal. Dormant identities increase the potential attack surface in the environment by providing attackers a greater number of access points to sensitive information. After all, any identity with access to data is a potential attack vector. Often dormant identities are from old employees or vendors. In worst case scenarios, organizations may have dormant identities with admin access, which are a gold mine for cyber threat actors if compromised. One of the easiest ways to compromise a dormant identity is leveraging compromised credentials from other data breaches. Dormant identities are less likely to be actively monitored and credentials rotated after a breach, allowing attackers to use the access to steal proprietary business information or manipulate data for personal gain. Often, if a dormant identity is compromised, the security team may be none the wiser.

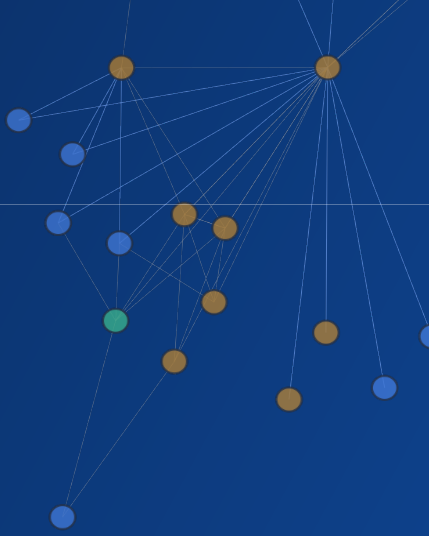
Remediations and Best Practices for Dormant Identities

To remediate dormant identities, Symmetry Systems recommends first setting priorities for the clean-up process, and then running an immediate risk-based, clean-up exercise. In each Zero Trust Data Assessment, Symmetry Systems arms businesses with a priority list of their riskiest dormant identities based on the identity's access to sensitive information or production data. DataGuard produces visual evidence, detailed analysis of previous activity, and guidance of what to review, clean up, and act on. This evidence includes additional risk factors, such as:

- **Whether Multifactor Authentication (MFA) is turned on or off.**
- **The reach of the identity through the environment.**
- **The sensitivity of the data that the identity can access.**
- **Existence of toxic combinations (access to discrete databases that overlap and allow for deeper access than actually intended).**
- **What operations can be performed by the identity against the data (delete, remove, etc.) and the risks if these operations are performed.**

The identification and prioritization of dormant identities is continuous, so our customers use DataGuard to assess their current environment to measure their enhanced data security posture and their reduction of cyber risk exposure over time.

As a next step, Symmetry Systems recommends building out internal procedures to further refine the timeframe of what indicates a dormant identity (time an identity goes unused to be considered dormant), and then using DataGuard to continuously monitor for and alert on new dormant identities. With the combination of process and alerts, security teams can keep a close eye on dormant identities and proactively reduce risk on an ongoing basis.



5. Over-Privileged Identities

What Are Over-Privileged Identities?

An over-privileged identity is an identity that has excessive ability to manage or control key functional and data elements of a system or infrastructure, compared to typical accounts, but doesn't actually use or need to have these assigned abilities. These types of identities have more privileges than are actually required to carry out job duties that are assigned to them.

Organizations tend to overestimate the level of access or permissions an identity actually needs to have. If compromised, over-privileged identities can result in significant and preventable business impact. For example, over-privileged identities may increase the risk of insider threat and supply chain attacks, especially if vendors or third parties can access data on more networks, systems, or data than they need.

How Do Over-Privileged Identities Happen?

Our Zero Trust Data Assessments universally find that customers grant too many permissions to a significant percentage of their identities. Typically, when new employees or vendors start, businesses tend to err on the side of granting permissions quickly and excessively to support business demand and operational need. Organizations also find it difficult to accurately define necessary permissions during employee or vendor onboarding.

Over-Privileged Identities: The Risks

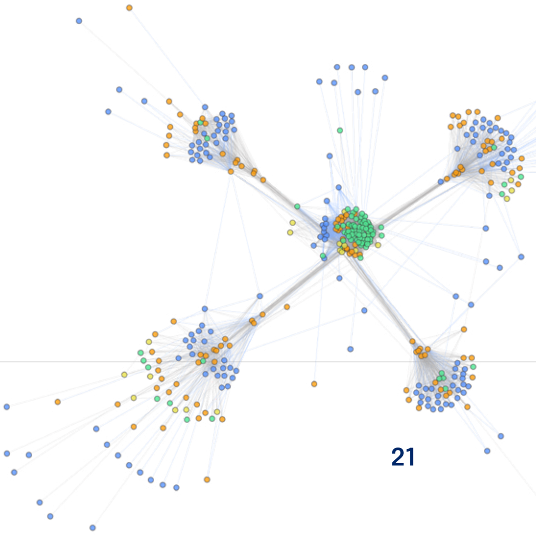
When identities are over-privileged or over-permissioned, the organization has granted a user potentially damaging access to and control over databases, systems, or applications. One problem we've frequently observed is over-permissioned identities may have the right to delete critical business data. Data deletion may happen intentionally or unintentionally, but the results are the same: significant disruption in business operations or technical environment. We've even observed that some over-privileged identities had the capability to create additional access keys! (Also known as a "silent hack.") With the ability to create access keys, these specific identities now have the ability to build paths to access data completely out of the purview of the security team, making it easy for that identity to hang onto access in the event that they left the organization or grant access to malicious parties outside of normal processes.

Over-privileged identities also pose a more significant risk if the identity is compromised because of the expanded blast radius from the excess privileges.

Remediations and Best Practices for Over-Privileged Identities

Symmetry Systems recommends that unused permissions be prioritized and then removed based on the same remediations and best practices outlined in the Dormant Identities section. In addition, to minimize the impact of compromise and reduce the attack surface and blast radius of a breach, a Zero Trust best practice is to only grant permissions in line with the identity's job duties and actual operational necessity. We also recommend that security teams build a streamlined and semi-automated process to remove permissions, only re-granting them when the identity requires the access to complete their job duties.

Permissions are relatively easy to both grant and remove. Organizations should consider implementing processes and technologies to enable time-boxed permissions to sensitive data and systems. With these procedures in place, security teams can reduce their attack surface and can enforce Zero Trust and least-privilege principles.



6. Delayed or Incomplete Employee and Vendor Offboarding

What Is Delayed or Incomplete Employee and Vendor Offboarding?

In order to keep up with the pace of business in our digital era, businesses grant access to data stores, technologies, applications, and other digital tools to their employees and third parties. Mismanaged vendor offboarding is when an organization ends a contract with an employee, vendor, consultant, business party, or other third party, but neglects to remove their access privileges to business systems.

How Does Delayed or Incomplete Employee and Vendor Offboarding Happen?

Businesses grant their employees access to data, systems, and applications. Organizations frequently grant access to consultants to repair, adjust, or enhance internal systems and applications. A vendor may get access to a specific data store, system, or application to help support an operational component–ranging from HR and help desk to HVAC. Organizations also frequently grant access to billing systems to business-specific partners or connect systems via API integrations. The relationship with these employees, consultants, vendors, and third parties tends to be owned by department champions, such as the CFO, HR, marketing, or procurement. In some cases, these department champions end relationships, but forget to notify the security team or the team that manages identity access permissions to remove access to systems or delete identities that no longer are required to conduct business. Often an organization may not have defined employee offboarding procedures, in which the security or information technology team is notified of employee departure. This results in former employees retaining their access to business systems.

Delayed or Incomplete Employee and Vendor Offboarding: The Risks

A compromised supply chain is the biggest risk associated with improper employee or vendor offboarding. Our engineers and scientists regularly find employee and vendor identities still active on customer systems, even though those individuals no longer work with the company. Upon further investigation, these often turn out to be departed vendors or employees that had not been properly offboarded. In some cases, we also find instances of third-party consultants who had been onboarded to complete projects on internal systems, but had since completed their contracts and moved on. In the case of the system consultants, while the individuals were no longer supporting the company and the accounts were clearly not in use, the identities were not only still active and lying dormant, but also still retained admin access rights!

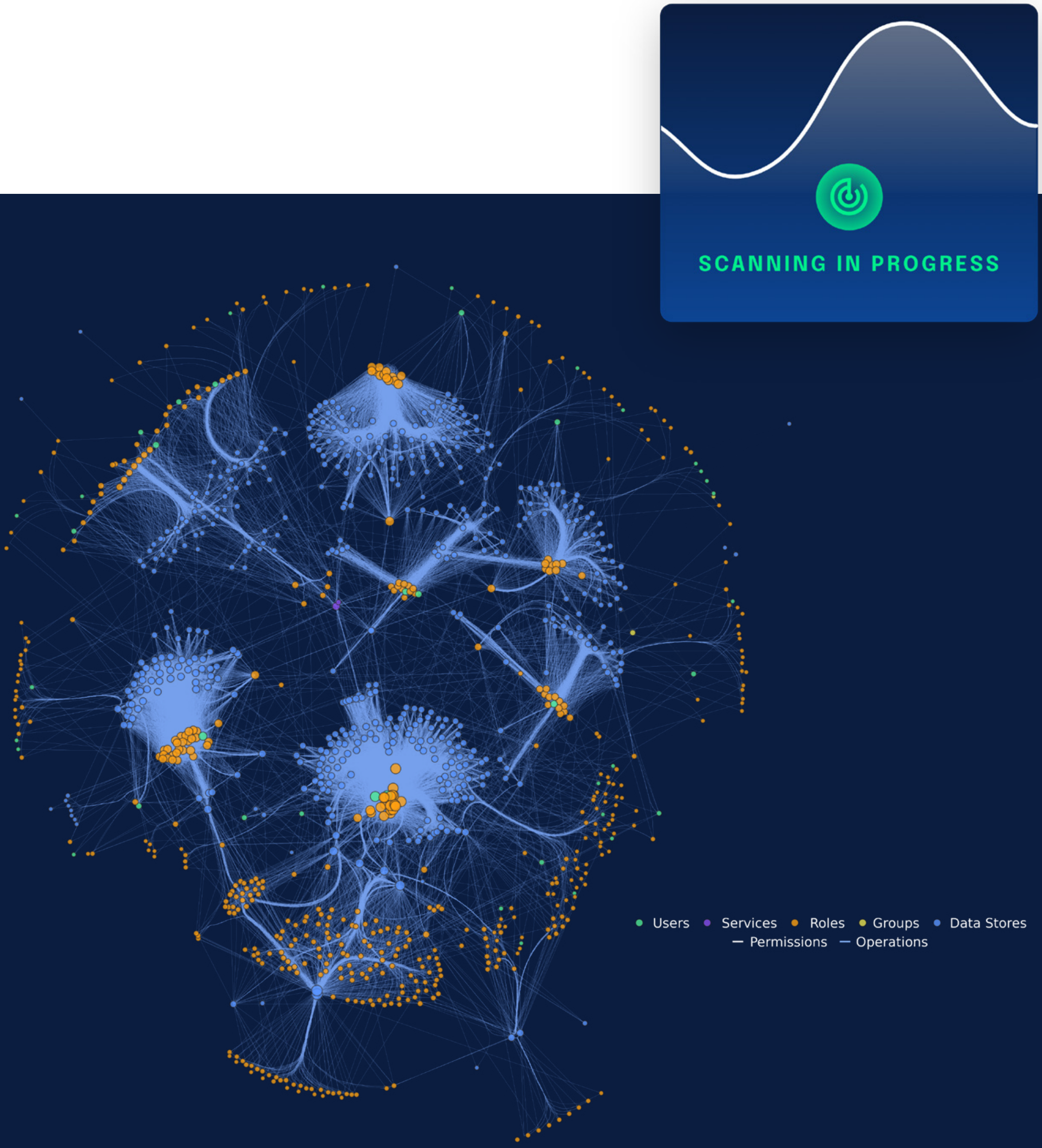
Symmetry Systems observed one specific example in which a security technology was deployed by a managed security service provider (MSSP). This provider still had an identity with access to the security tool and, because they initially deployed it for the organization, retained full control and access. Once deployed, the MSSP no longer needed access, yet, this improperly offboarded vendor retained full access to the entire environment.

In the scenarios we mentioned above, the end result could be malicious actors–cybercriminals or disgruntled employees–gaining improper and unauthorized access to systems and then causing some sort of disruption or engaging in a criminal act. If a threat actor has acquired an unused/inactive identity, they could potentially gain read, edit, delete, and run operations on data in the entire environment. Similarly, malicious employees might use their access in harmful ways like vandalism and stealing sensitive information. Even improperly offboarded (but non-malicious) employee identities present risk, because if these identities become dormant, threat actors might be able to use them to gain access to sensitive or mission critical data. Ultimately, if organizations do not have processes and policies in place to immediately and effectively offboard vendors and employees, the organization's attack surface grows.

In order to protect your organization from cyber threats and attacks, you need to know what you have to protect (data), who to protect it from (threat actors and malicious insiders), and how the identity or technology could be used as a proxy to gain access to what you are trying to protect. If external identities that no longer have an active business relationship with an organization can still access the data and can execute on tasks using that data, you are leaving doors wide open for threat actors or malicious insiders.

Remediations and Best Practices for Incomplete Employee and Vendor Offboarding

Symmetry Systems recommends that organizations assess the effectiveness of their cross-team or interdepartmental workflows, policies, and procedures to make sure all employees and vendors are properly offboarded. The team that manages identity access management should be notified immediately so that they can adjust identities and access rights and reduce the number of unused employee and vendor accounts at risk. Continuous monitoring to alert security teams of potential process failures to remove these accounts is also extremely important.



7. Inadequate Segregation of Duties Between Development, Test, and Production Environments

What Is Inadequate Segregation of Duty?

Segregation of duty, also known as separation of duties, is a concept in which an organization breaks down an end-to-end process into discrete tasks that no single identity or individual can complete on their own. Organizations do this so that no single identity, technology, or individual has full control over the task. Generally speaking, organizations deploy segregation of duty to reduce the risk of data fraud, misuse, theft, sabotage, and other potential security challenges. The most effective segregation of duty is to ensure that development, test, and production environments are separate.

How Do Inadequate Segregation of Duty Problems Happen?

Across the Zero Trust Data Assessments that Symmetry Systems conducts, we find that organizations infrequently enforced segregation of duties between development, test, and production environments as a control or security mechanism when securing data. The overlooking of segregation of duties is a common oversight during the adoption of DevOps practices. Most concerning, we found that many organizations had not deployed guidelines, policies, or procedures to enforce data flow boundaries between their environments. Organizations continually exhibit blurred lines between development, staging, and production environments.

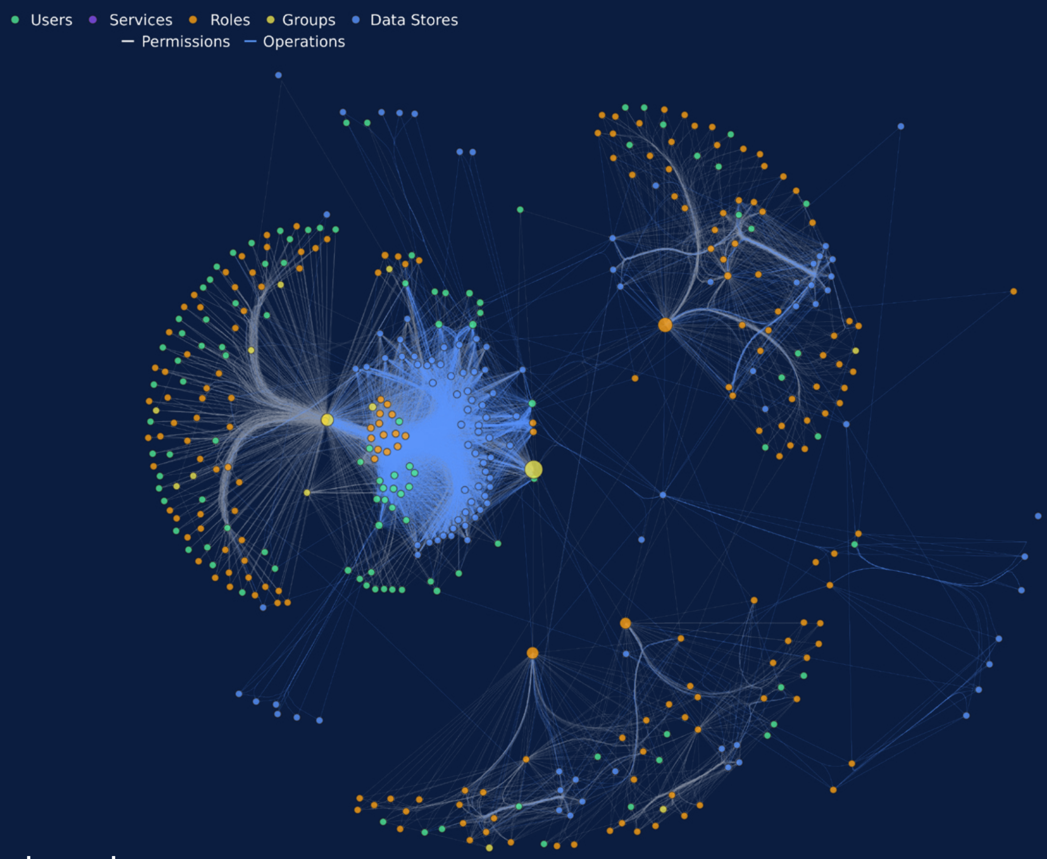
Inadequate Segregation of Duty: The Risks

Ultimately, the biggest risk for companies with an inadequate segregation of duty process is that it increases the likelihood of sensitive data access by unauthorized parties. It also allows identities to easily move data between data stores at will, without benefit of security controls, which contributes to data leakage and loss. Inadequate segregation of duty further expands both the attack surface and data blast radius if a security incident were to occur.

Remediations and Best Practices for Inadequate Segregation of Duty

Enforcing segregation of duty, particularly through the boundaries that exist between environments, is an important security measure organizations should deploy to reduce the risk of data leakage and data loss. Data should never be allowed to leave an environment without clear business-approved rationale and without a specifically designed identity that is strictly controlled.

We recommend that no single identity be granted the permission to access production, staging, and development environments. We also recommend that these roles be refactored to ensure permissions are maintained at a granular level to minimize the impacts of cross-account data flows. (Unfortunately cross–account data flows are a leading cause of data leakage out of data stores, and hence these cross–account data flows must be closely monitored and controlled.) By breaking up roles and identities into smaller pieces with more granular permissions, organizations can limit the impact and minimize the risk of data leakage and loss. Organizations also need to ensure that production data cannot be used for testing purposes, because when placed in insecure testing environments the risk of the data being accessed by unauthorized parties is increased.



8. Application and Backup Misconfiguration

What Are Application and Backup Misconfigurations?

Application and backup misconfigurations are when security, development, or engineering teams install new or modify existing technologies, services, and cloud data stores and do not configure them properly or fail to configure with reducing security risks in mind.

Misconfigurations can include everything from:

- **Not changing default usernames and passwords.**
- **Enabling hard-coded backdoor accounts.**
- **Leaving special access mechanisms running.**
- **Setting incorrect permissions for identities.**
- **Not enabling scheduled data backups.**
- **Setting incorrect permissions for data access through web servers.**
- **Numerous other types of scenarios.**

How Do Application and Backup Misconfigurations Happen?

Ultimately application and backup misconfigurations can be traced back to user error, inadequate knowledge or incomplete configurations. Security, development, and engineering teams tend to be under tremendous pressures to complete projects and ship finished products on time. This high-intensity working environment can breed human error. During assessments, our engineers uncover a wide array of misconfigurations that open doors for data loss, data leakage, and threat actor access. In most cases, the issues could have been avoided with correct configurations. A few specific misconfigurations we seen include:

- **Granting access to unnecessary or unused features, thereby expanding the attack surface.**
- **Inadequate access controls.**
- **Unprotected files and directories.**
- **No scheduled or failed data backups.**

Application and Backup Misconfigurations: The Risks

Misconfigurations–in applications, technologies, and datastores–create noise, which means that the team that manages the systems gets bombarded with error messages that they need to sift through. Misconfigurations also lead to failed operations, which can be used by threat actors to access sensitive locations within a system. Without visibility into datastores, most organizations don't see the full extent of misconfigurations or any bad actors that might already be embedded.

We find that many organizations opt to turn off data activity monitoring (DAM) entirely because they are inundated with these alerts and error messages. If the organization has deployed DAM technologies, the amount of alerts and logs generated from misconfigured systems will be too large of a burden for most teams. And should a worst-case scenario happen and a data breach occurs, the incident response team will spend valuable time chasing false positives, rather than thwarting a specific threat.

In addition, application-based configuration files that are not secured properly may reveal clear text connection strings to databases. This can lead to unauthorized access of sensitive information or mission critical data. Ensuring that data stores and technologies that access them are configured with security in mind is paramount.

Remediations and Best Practices for Application and Backup Misconfigurations

While there are best practices every business can take to avoid misconfigurations, we're all still human. It's critically important to recognize that misconfigurations are going to happen and to search for and identify them regularly and often. Symmetry Systems DataGuard automatically unearths misconfigurations in every customer data environment. DataGuard then flags the misconfiguration to enable the business to take action. By telling the security team which misconfigurations in which technologies to review and address, DataGuard helps to proactively fortify an organization's data security posture.

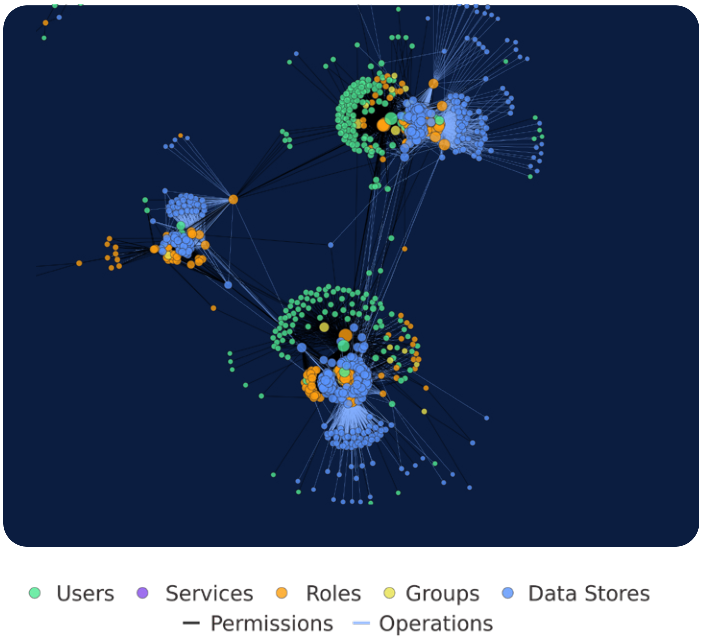
From there, DataGuard can help narrow down false positive alerts, hone in and monitor for future misconfigurations that might arise, and facilitate receipt of timely alerts via Slack or CloudWatch integrations on any user error or system changes that need to be reconfigured with security in mind.

Data Collection, Analysis, & Reporting in DSPM and DataGuard

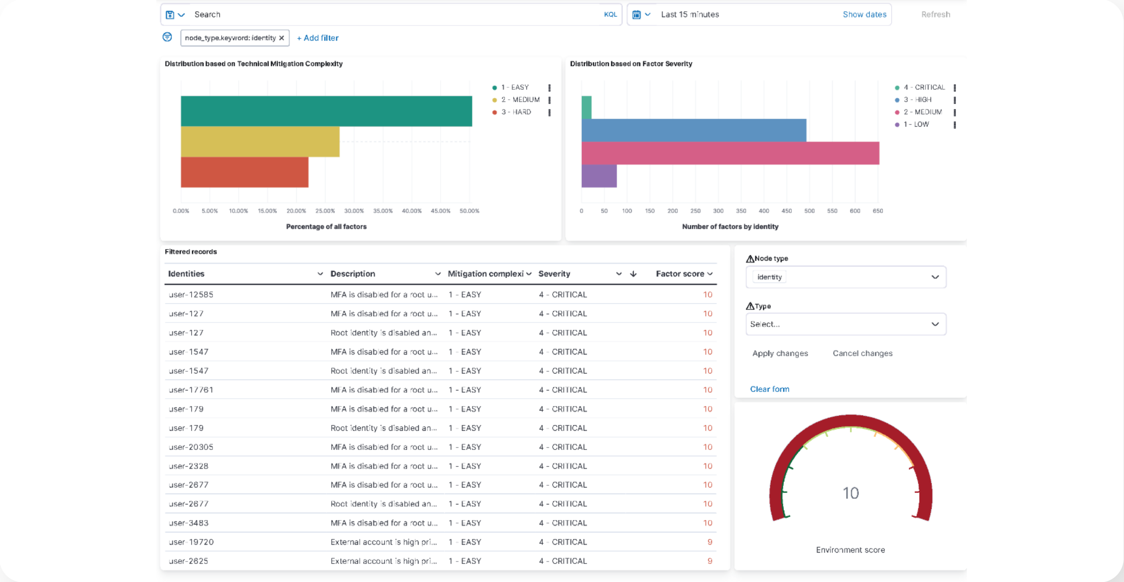
DataGuard is purpose-built to make it easier for businesses to secure data at scale. DataGuard delivers tangible advice on how to significantly reduce the impact and frequency of data breaches, minimize the attack surface, lower cyber security risks, reduce data sprawl, and support effective Zero Trust deployment efforts. Symmetry hybrid-cloud engineers developed DataGuard to quickly deploy in Amazon Web Services, Microsoft Azure, Google Public Cloud, and on-premises environments. DataGuard performs agentless scans in customer environments, with data never leaving the customer environment.

Once deployed, DataGuard:

1. Builds an accurate data inventory and visual representation of the customer's data objects, identities, and all permissions and actions taken on the data objects by identities.
2. Classify data within the customer's data inventory.
3. Identifies least privilege issues by analyzing actions and permissions across AWS, GCP, Azure, and on-premise deployments.



4 Conducts a machine learning-driven graph analysis that prioritizes areas of greater categorical and overall data risk across datastores and then pinpoints any identities accessing them.



node_type.keyword: identity

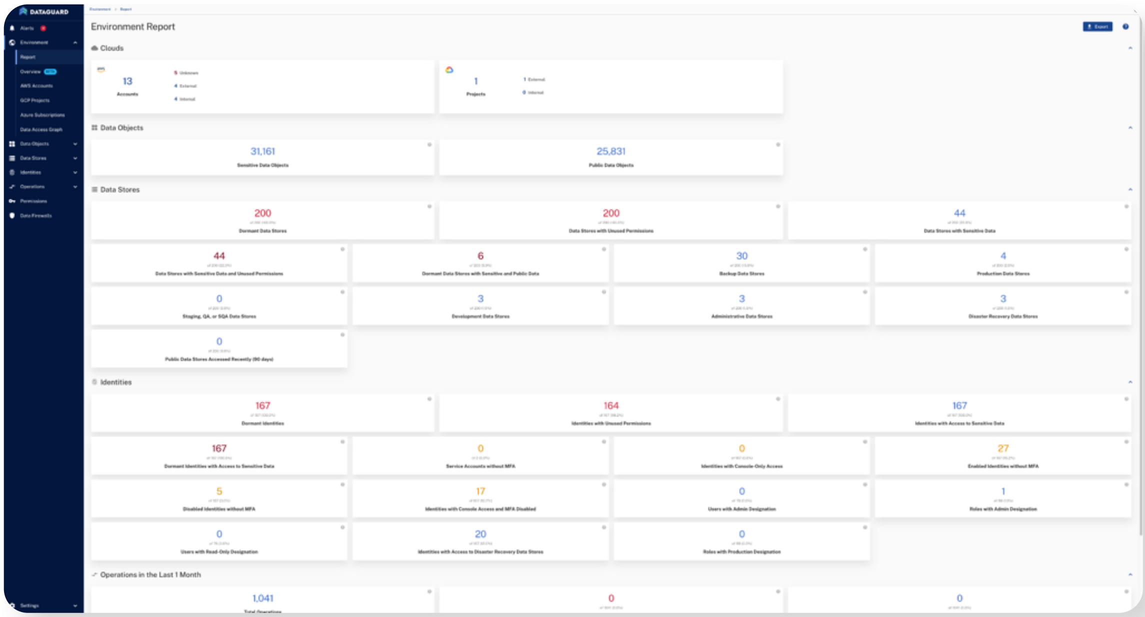
Filtered records

Identities	Description	Mitigation complexi	Severity	Factor score
user-12585	MFA is disabled for a root u...	1 - EASY	4 - CRITICAL	10
user-127	MFA is disabled for a root u...	1 - EASY	4 - CRITICAL	10
user-127	Root identity is disabled an...	1 - EASY	4 - CRITICAL	10
user-1547	MFA is disabled for a root u...	1 - EASY	4 - CRITICAL	10
user-1547	Root identity is disabled an...	1 - EASY	4 - CRITICAL	10
user-17761	MFA is disabled for a root u...	1 - EASY	4 - CRITICAL	10
user-179	MFA is disabled for a root u...	1 - EASY	4 - CRITICAL	10
user-179	Root identity is disabled an...	1 - EASY	4 - CRITICAL	10
user-20305	MFA is disabled for a root u...	1 - EASY	4 - CRITICAL	10
user-2328	MFA is disabled for a root u...	1 - EASY	4 - CRITICAL	10
user-2677	MFA is disabled for a root u...	1 - EASY	4 - CRITICAL	10
user-2677	Root identity is disabled an...	1 - EASY	4 - CRITICAL	10
user-3483	MFA is disabled for a root u...	1 - EASY	4 - CRITICAL	10
user-19720	External account is high pri...	1 - EASY	4 - CRITICAL	9
user-2625	External account is high pri...	1 - EASY	4 - CRITICAL	9

⚠Node type: identity

⚠Type: Select...

5 Identifies and prioritizes potential data security, compliance and privacy, and IAM gaps that should be addressed to reduce cyber risk.



Environment Report

Clouds

13 Accounts — 5 Unknown, 4 External, 4 Internal

1 Projects — 1 External, 0 Internal

Data Objects

31,161 Sensitive Data Objects

25,831 Public Data Objects

Data Stores

200 Dormant Data Stores

200 Data Stores with Unused Permissions

44 Data Stores with Sensitive Data

44 Data Stores with Sensitive Data and Unused Permissions

6 Dormant Data Stores with Sensitive and Public Data

30 Backup Data Stores

4 Production Data Stores

0 Staging, QA, or SQA Data Stores

3 Development Data Stores

3 Administrative Data Stores

3 Disaster Recovery Data Stores

0 Public Data Stores Accessed Recently (90 days)

Identities

167 Dormant Identities

164 Identities with Unused Permissions

167 Identities with Access to Sensitive Data

167 Dormant Identities with Access to Sensitive Data

0 Service Accounts without MFA

0 Identities with Console-Only Access

27 Enabled Identities without MFA

5 Disabled Identities without MFA

17 Identities with Console Access and MFA Disabled

0 Users with Admin Designation

1 Roles with Admin Designation

0 Users with Read-Only Designation

20 Identities with Access to Disaster Recovery Data Stores

0 Roles with Production Designation

Operations in the Last 1 Month

1,041 Total Operations

0

0

Conclusion

Information is everywhere. It's in the cloud. It's stored on-prem. Vendors can access it and copy it outside your control. Applications retain it. Managing and securing this vast load of data is complex. There are millions of data objects across thousands of data stores, multiplied by a seemingly infinite combination of roles and permissions for thousands of user and machine identities. Add to this layers of security solutions, each designed to protect a single aspect of the systems around the data, which range from creating and securing a perimeter to detecting malware, all easily circumvented by compromising access and identities.

It's no wonder businesses struggle to properly inventory, classify, control, and protect their critical data assets, while at the same time securing this data from attacks, insider threats, third-party supply chain attacks, vendor threats, and data breaches. If all of this weren't enough, there is also the added complexity of governance and compliance due to evolving data privacy and security regulations and mandates.

Today's businesses are required to store and secure different types of data across complex cloud and on-premises infrastructures. Data protection can no longer begin and end at the perimeter or the devices being used. SecOps, information security, data, and IT teams must be enabled with information that tells them where data resides, how sensitive it is, who has access, and how that data is being used.

It's called full data visibility. And it's what Symmetry Systems DataGuard is all about.

If you're ready to secure data more effectively than your current patchwork of traditional security tools like data loss prevention (DLP), data activity monitoring (DAM), and cloud infrastructure entitlement management (CIEM), let's talk.

It's time to replace these outdated models and products with a comprehensive Data Security Posture Management (DSPM) solution that extends the Zero-Trust philosophy to hybrid-cloud data stores. Secure your business from the data out. Schedule a DataGuard demo now.

Ready to secure your data with precision and scale?

Stop chasing threats at your perimeter.
Know your data security posture and protect your mission critical data.

For more information, visit us at **www.symmetry-systems.com**