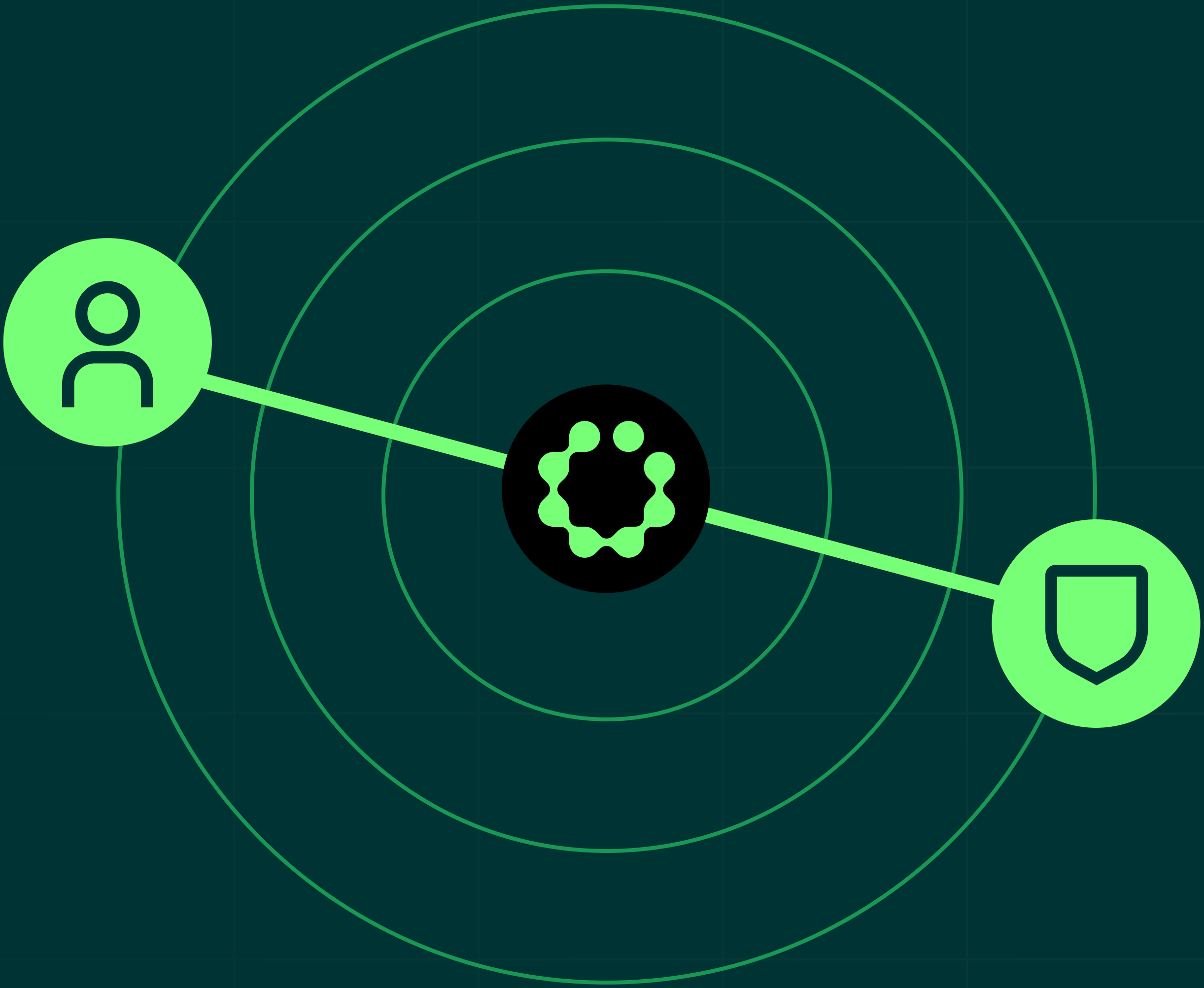
CYERA

INDUSTRY WHITEPAPER

Data and Identity

The Evolving Security Paradigm



Executive Summary

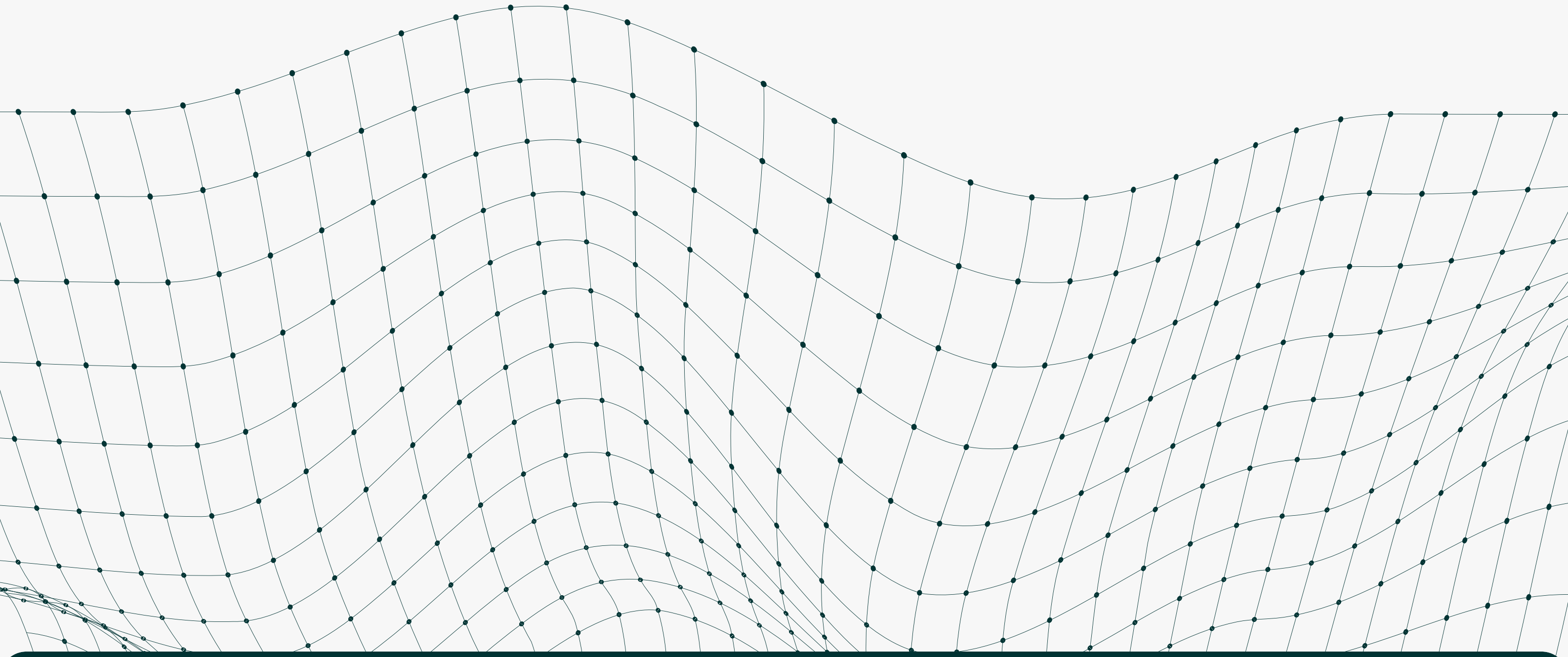
As organizations continue to digitize and migrate operations to the cloud, developers continue to write code and develop software, and non-human entities proliferate, the volume of data generated, and managed, has grown exponentially. It is estimated that by 2025, the global dataverse will grow to over 181 zettabytes of data.

Concurrently, the adoption of AI services is expanding, with 72% of companies reporting current usage within their organizations. This is dramatically changing not just the enterprise environment - but the entire world. According to Gartner by 2026, 50% of governments worldwide will enforce use of responsible AI through regulations, policies and the need for data privacy.

This surge in data, and rapid AI adoption, has led to an alarming rise in security risks - of which users, both internal and external, as well as non-human identities (NHI), remain the greatest threat to business security. The criticality of Identity Access Management (IAM) is not new to security organizations - hence the success of companies like Okta, Microsoft, and others who are known for their IAM services. However, very little has been explored, or even talked about, when it comes to the relationship between identity and data.

What's clear is that data and identity have emerged as the two fastest-growing security attack surfaces. Yet, aligning these two elements within a security framework has proven to be a significant challenge - despite the shared responsibility model in cloud environments which clearly states that both data and identity are the responsibility of the enterprise, and not the cloud service provider. Security teams struggle to integrate data and identity protection due to a variety of challenges - most notably siloed processes, disparate services, and weak data discovery and classification capabilities.

This whitepaper outlines the pressing need for organizations to align data and identity protection in the face of growing security challenges. By adopting an integrated approach, security leaders can enhance their overall security posture and protect their most valuable asset - data. In this piece we explore the evolving security landscape, the challenges faced by security teams, and provide an activity guide to help improve the way you approach identity and data security.

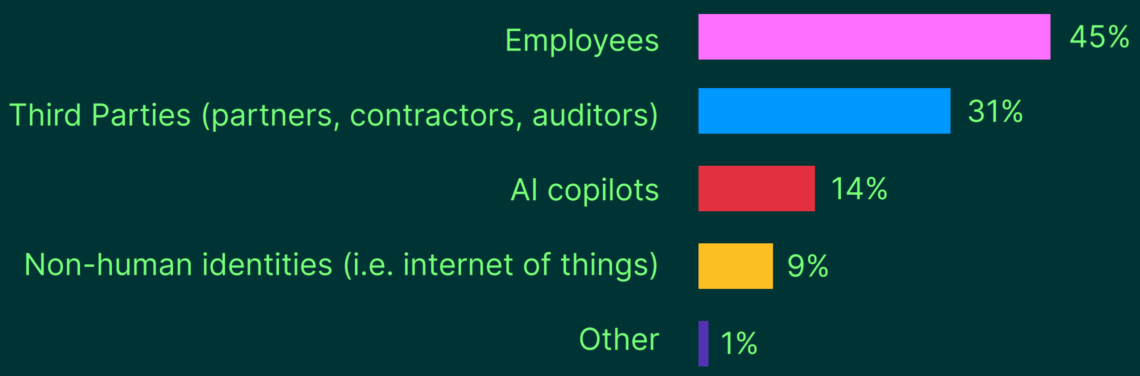


The Growing Security Challenge

The Rise of Data and Identity as Attack Surfaces

Data and identity have become the primary targets for cyberattacks, driven by the exponential growth in data volumes and the increasing complexity of identity management. While, one could argue that data has always been the main target for a data breach, what's changed is the advent of tools like AI, which have access to large amounts of enterprise data, and if scaled irresponsibly, increases the probability of danger. This makes for the perfect storm when combined with the fact that identity has been the main entry point given the inevitable reality that people will always be the weakest link in the security chain. Social engineering attacks, inconsistent use of multi-factor authentication, inability to evoke zero trust principle of least privilege access, or third-party suppliers accessing the network via VPN.

What entities are you most concerned about from a data security perspective?



The Human and Non-Human Identity Factor

Understanding the types of identities operating within the environment is critical. These span both human as well as non-human identities (NHI). Below is a brief description of each.

Human Identities

Human identities include employees and third parties, which have traditionally been the focus of identity management. However, the rise of AI and other non-human identities has added a new layer of complexity to identity management.

Employees

Employees, particularly those with access to sensitive data, pose a significant security risk. For example, in the Snowflake environment, managing employee access to sensitive data requires a robust identity management system that can identify and mitigate potential risks.

Third-Parties: Contractors & Partners

Vendors, contractors, auditors and other partners often have access to sensitive data, creating additional security risks. The risk is further compounded by the "Nth Party" phenomenon, where third-party vendors subcontract work to other vendors, creating a complex web of access points that are difficult to manage.

Non-Human Identities (NHI)

Non-human identities include AI services, SaaS applications, and services exposed to the internet. These are becoming increasingly prevalent in today's digital landscape. These identities require the same level of scrutiny and management as human identities.

AI Services

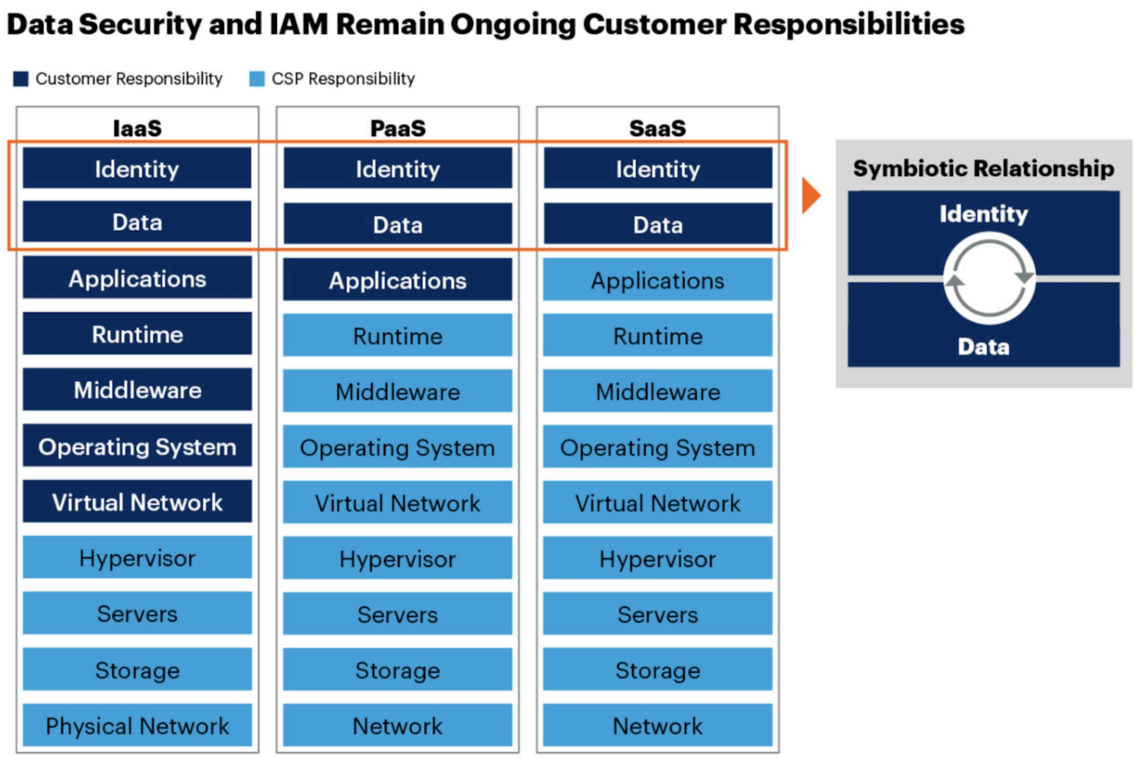
By 2027, organizations will standardize on policy-based access controls to unlock the value from more than 70% of their data, according to Gartner. As AI services, like AI Copilots from Microsoft, Salesforce, Amazon, Google and others continue to evolve, organizations must ensure that these services have appropriate access controls to prevent unauthorized access to sensitive data.

SaaS Applications and Internet-Exposed Services

SaaS applications and services exposed to the internet also pose significant security risks. These applications often require access to sensitive data, making them a prime target for cyberattacks. They can also pass along sensitive data to other SaaS applications as well. Security teams must implement robust identity and access management (IAM) controls to protect these applications and services.

Breaking down silos between data and identity security

The traditional approach to security treats data and identity as distinct entities, each with its own set of protection mechanisms. This siloed approach has resulted in fragmented security processes, making it difficult for security teams to gain a comprehensive view of their security posture.
Additionally, the lack of robust data discovery and classification tools further complicates the alignment of data and identity protection. As organizations adopt cloud services, they inherit the responsibility of securing both data and identities under the shared responsibility model.



Data Security and IAM Remain Ongoing Customer Responsibilities

■ Customer Responsibility ▨ CSP Responsibility

IaaS	PaaS	SaaS
■ Identity	■ Identity	■ Identity
■ Data	■ Data	■ Data
■ Applications	■ Applications	▨ Applications
■ Runtime	▨ Runtime	▨ Runtime
■ Middleware	▨ Middleware	▨ Middleware
■ Operating System	▨ Operating System	▨ Operating System
■ Virtual Network	▨ Virtual Network	▨ Virtual Network
▨ Hypervisor	▨ Hypervisor	▨ Hypervisor
▨ Servers	▨ Servers	▨ Servers
▨ Storage	▨ Storage	▨ Storage
▨ Physical Network	▨ Network	▨ Network

Source Reference: Gartner

However, aligning data and identity protection remains a daunting task. Amid this shift, it’s crucial to recognize that while many security responsibilities are transferred to cloud providers, the protection of data and the management of access remain the end customer's responsibility across all cloud service delivery models—whether IaaS, PaaS, or SaaS. Consequently, data security and Identity Access Management (IAM) continue to be core responsibilities for customers. This ongoing responsibility is driving an interesting evolution: data security and IAM are increasingly converging into a more integrated relationship.

This convergence is both reflected in and driven by market trends and changing demand dynamics. Enterprises often struggle with managing data security, data management, and IAM as separate, isolated entities. As organizations mature, they're realizing that treating these disciplines in isolation often results in inefficiencies and suboptimal outcomes. Data security requires IAM as part of its protect surface, while IAM cannot provide comprehensive access control without robust data security insights and high-precision data classification - which is key for determining the criticality of sensitive data and the correlation between identity and data. By combining these efforts, organizations can tackle long-standing challenges that arise from siloed approaches - and usher in a new security framework that combines data security and identity security into a unified strategy. The future of IAM, data management, and data security is undoubtedly intertwined, and soon they will be viewed as inseparable.

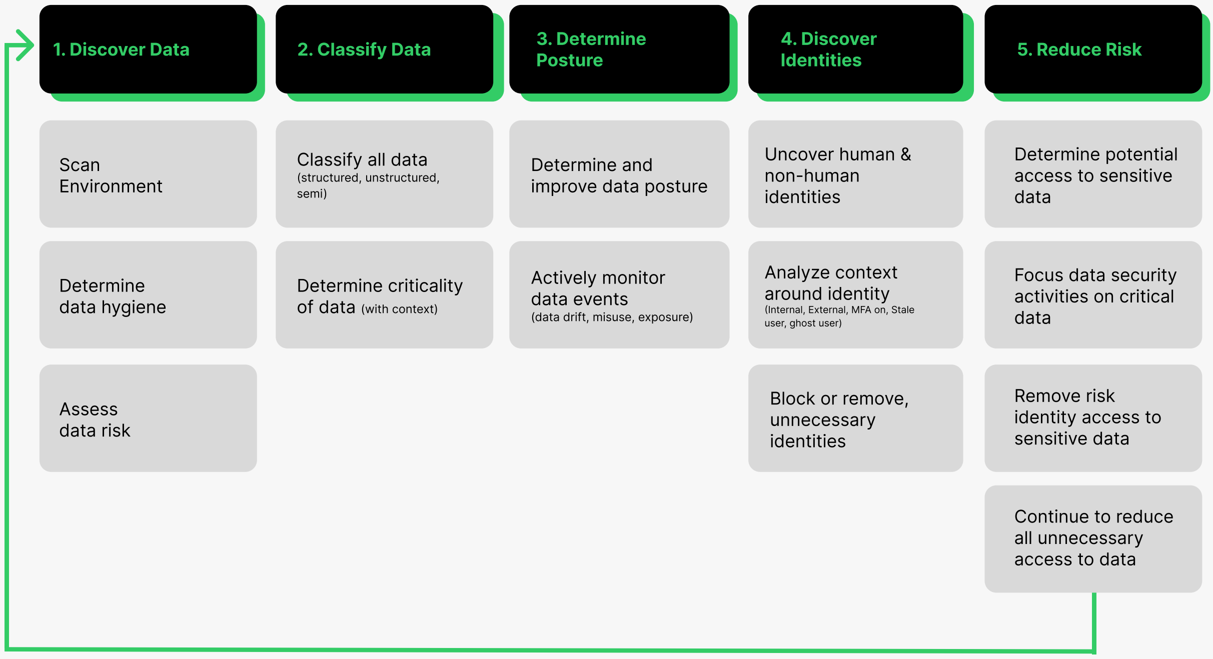
The co-evolution of data security and IAM marks a significant shift in safeguarding sensitive data and managing user access across hybrid environments. As SaaS, IaaS, and DBaaS continue to redefine the cybersecurity landscape, and extend the corporate perimeter beyond the datacenter, data security and IAM will be the critical cornerstones. Together, they will shape the future of customer-managed security controls, ensuring not only protection but also the effective and responsible management of higher-order risks, such as insider threats.

To address the growing security challenges, organizations should integrate data security with identity access management. Data security teams need to shift their focus from asking "Where is my sensitive data?" to "Who or what has access to it?" Similarly, identity managers must consider not only which identities are operating within their environment but also what data these identities can access.

For example, consider a scenario where OneDrive is compromised for the top 20 executives of an organization. Security teams must be able to quickly determine what data was impacted, who had access to it, and whether a compliance violation occurred. The ability to assess the materiality of the breach and its potential cost is crucial for minimizing the impact of such incidents.

Below is an activity guide that we developed for our customers here at Cyera. This provides a roadmap for security leaders looking for a way to ensure the co-evolution of data and identity security.

Activity Guide for Data & Identity Security



1. Discover Data	2. Classify Data	3. Determine Posture	4. Discover Identities	5. Reduce Risk
Scan Environment	Classify all data (structured, unstructured, semi)	Determine and improve data posture	Uncover human & non-human identities	Determine potential access to sensitive data
Determine data hygiene	Determine criticality of data (with context)	Actively monitor data events (data drift, misuse, exposure)	Analyze context around identity (Internal, External, MFA on, Stale user, ghost user)	Focus data security activities on critical data
Assess data risk			Block or remove, unnecessary identities	Remove risk identity access to sensitive data
				Continue to reduce all unnecessary access to data

The Need for Modern Data and Identity-Centric Security Solutions

As the security landscape evolves, it is imperative for organizations to rethink their approach to data and identity protection. There is a critical need for more education on the interconnectedness of data and identity. Security teams must recognize that data and identity are not distinct but rather interconnected elements that should be protected as part of a unified security strategy. Security leaders must understand the positive value this interconnectedness brings to the business, including improved identity discovery, least-privileged access, and safer AI adoption without increasing business risk.

But vendors also play a crucial role in helping organizations achieve these goals. They must develop solutions that enable customers to determine the critical data and identities operating within the company, determine access context, and take steps to remediate and minimize unnecessary access. These capabilities are essential for aligning data and identity protection within a unified security strategy.

Emerging technologies like Data Security Posture Management (DSPM) are gaining traction as they offer a more integrated approach to data and identity protection. Often part of a larger Data Security Platform (DSP), DSPM technologies allow organizations to identify and mitigate security risks by providing visibility into sensitive data across all environments, and aligning it with the identity discovery and access services that are now offered by some DSPs. Below are some of the identity-centric use cases that DSP services support.

1. Discover identities within your environment - discovers identities across your landscape and determines a trust level for each identity. This trust level is either external, external-trusted, or organizational

2. Understand the context in which that identity has access to the data - Identify whether this entity was internal or external, human or non-human, did they have MFA turned on, were they ghost users, or stale users. This context is key given the cyber attacks that now exploit this context like in the case of Snowflake.

3. Reduce over privileged access - Gain insights to determine whether or not access to the data is actually required - and correlate this with the sensitivity levels of this data, as well as number of total records. Then take action to reduce any unnecessary access to data.

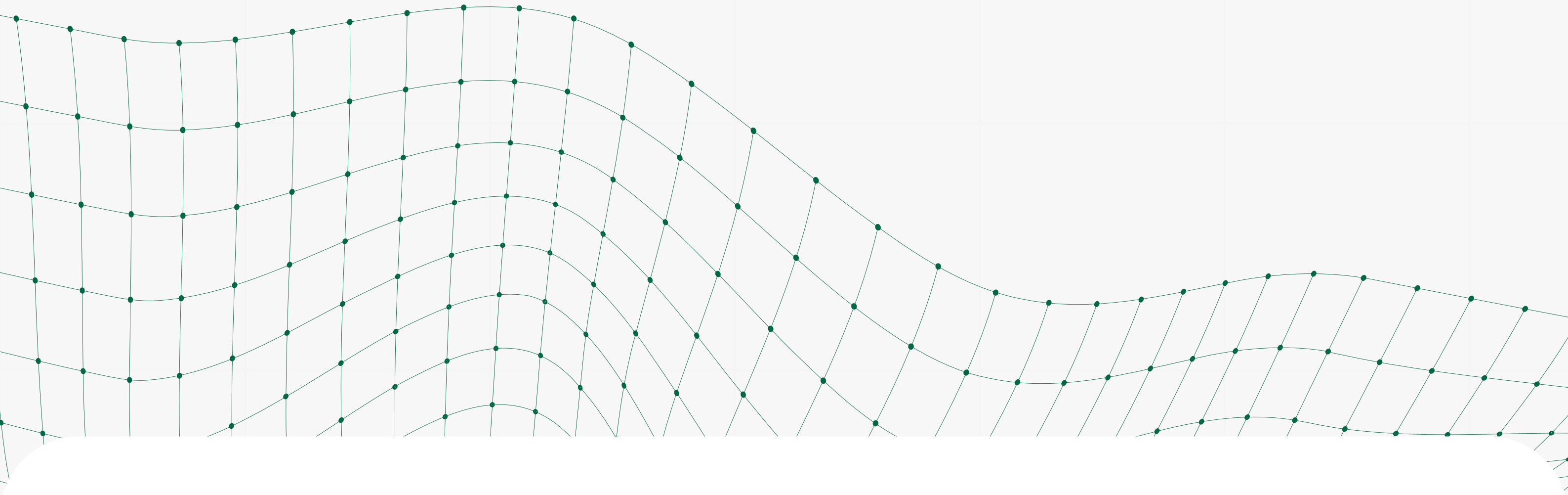
4. Control the AI blast radius - Discover if Microsoft Copilot, or AWS Sagemaker, a GenAI platform, has access to PII data, employee compensation information, intellectual property (the secret recipe) or any other sensitive data. Then use this insight to reduce an AI data breach.

The Need for Modern Data and Identity-Centric Security Solutions

Continued

Security leaders, and their teams, must adapt to the changing threats posed by data and identity. By recognizing the interconnectedness of these two elements and integrating their protection within a unified security strategy, organizations can better protect their sensitive data and identities. As new technologies like DSPM, and DSP, gain traction, security leaders must embrace these solutions to stay ahead of the evolving threat landscape. The future of security lies in the seamless integration of data and identity security, and organizations must act now to safeguard their digital assets.

To learn about our approach here at Cyera feel free to request a demo at https://www.cyera.io/demo



About Cyera

Cyera is reinventing data security. Companies choose Cyera to improve their data security and cyber-resilience, maintain privacy and regulatory compliance, and gain control over their most valuable asset: data. Cyera instantly provides companies with a holistic view of their sensitive data and their security exposure, and delivers automated remediation to reduce their attack surface.

Learn more at **www.cyera.io**, or follow Cyera on **LinkedIn**.

Trusted by:

SKECHERS | PELOTON | CHIPOTLE | AT&T | BlueCross BlueShield

Takeda | Constellation Brands | DELTA DENTAL | Rockwell Automation | Tyson Foods