Normalyze®

data-first cloud security

Normalyze

Data Security Posture Management

Securing your data ... **wherever it is.**

Content

Overview 2

Unique platform capabilities 3

1. Discovery and classification of data wherever it is 3
2. Prioritization of datastores 3
3. Achieve least privilege access to data stores with ease 4
4. Attack path detection and guided remediation 4
5. Compliance mapping and reporting 4
6. DSPM for AI 4
7. DSPM for Snowflake 4

Normalyze architecture 5

Supported platforms and technologies 6

Learn More 6

Gen AI is leading to more sophisticated social engineering attacks, with deepfake attacks becoming increasingly prevalent.

the cost of cyberattacks on the global economy, by the end of 2024 **$10.5T**

83%

of organizations having experienced at least one breach related to access issues.

Source: https://www.pingsafe.com/blog/cloud-security-statistics/

$4.35M is the average cost of a data breach… with public cloud breaches being more expensive than hybrid cloud breaches.

Overview

We are witnessing an **unprecedented explosion in data** driven by the advent of Generative AI, expansive data lakes, and the widespread adoption of cloud technologies. This surge in data volume and complexity has resulted in a loss of visibility and control for enterprises. Even with thousands of security tools in the market, **data breaches continue to occur daily**. Compounding the challenge, the traditional data security approaches struggle to keep pace with the evolving landscape.

To solve these issues, Normalyze takes a **data-first approach** to security. Normalyze is the pioneer of Data Security Posture Management (DSPM), helping enterprises secure their data across SaaS, PaaS, public or multi-cloud, on-prem and hybrid environments. With Normalyze, security and data teams can improve their overall security and compliance efforts while empowering the business to leverage their most precious asset: data.

The Normalyze DSPM platform helps to discover and classify data stores, prioritize what's important, identify risky and excessive access, detect and remediate exposure risks, and improve compliance and auditing processes.

At the heart of the Normalyze platform is the patented One-Pass Scanner™, which leverages AI to accurately identify and classify valuable and sensitive data at scale, across different environments.

The platform was designed around an architecture that scans in place, so data never leaves the location where it resides.This approach keeps data under IT control, supports compliance with stringent data protection regulations and enhances operational efficiency.

Scanned results appear in multiple visualizations to help teams prioritize risk. The Data Risk Navigator™ shows attack paths that can lead to data breaches or loss. Data Access Graphs shows how people and resources access data. Visualizations are generated and updated in real time, providing visibility as changes to customer infrastructure or environments take place. The proprietary DataValuator™ assigns monetary value to data, with a ranking to help security and data teams assess the relative business impact of potential data loss.

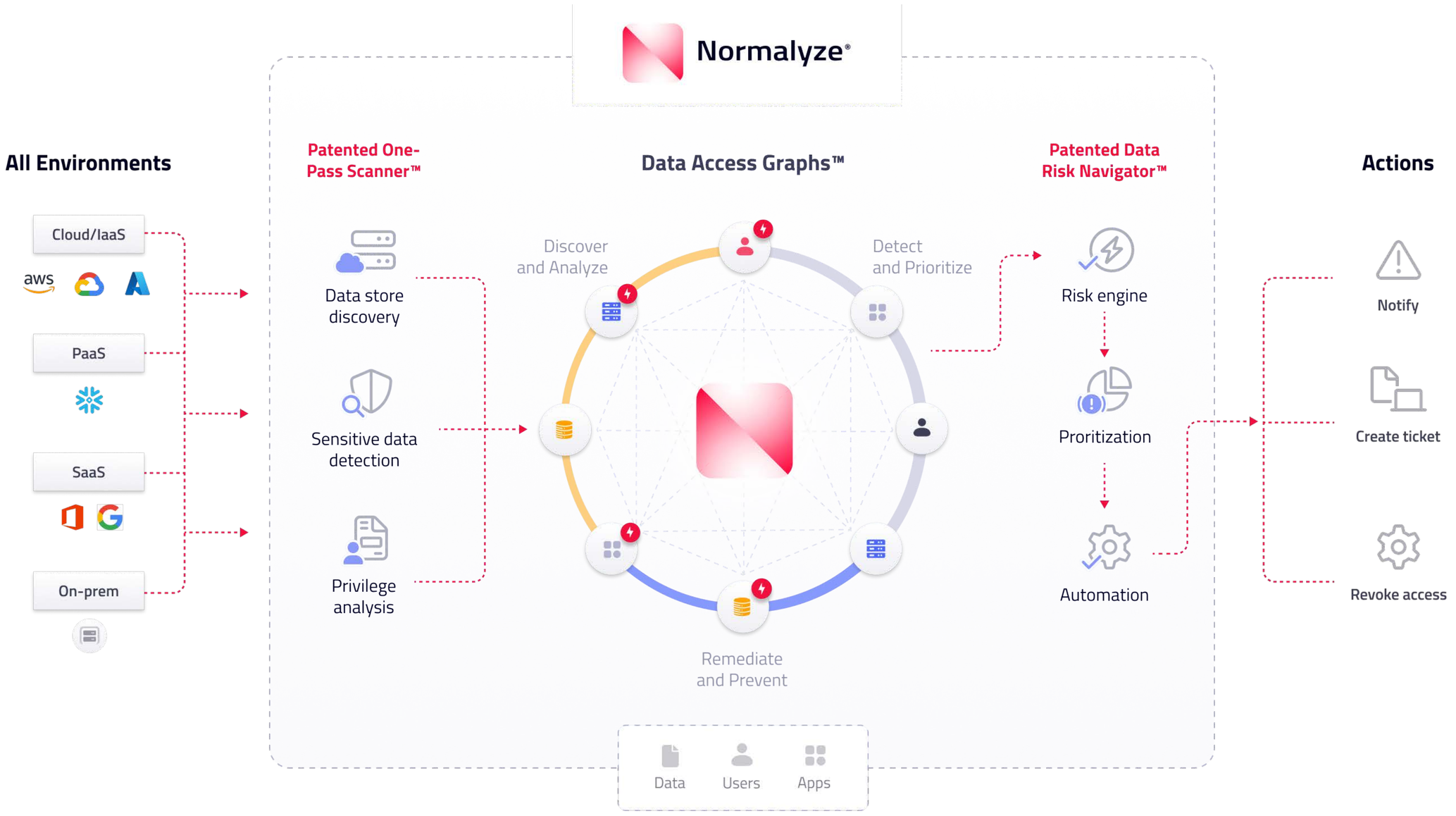
AI-powered querying and remediation workflows make the Normalyze user experience intuitive and efficient. Delivering insights into data, access, and risk in one place, IT teams can understand their overall data security posture, and collaborate on effective security measures and action plans.

Unique Platform Capabilities

AI-powered data discovery and classification

Patented data attack path detection

Prioritized risks with AI-guided remediation



Discover and classify data wherever it is

Normalyze constantly discovers new datastores as they are instantiated in your ever-changing data environments. Using the patented One-Pass Scanner, Normalyze provides the most accurate classification of data in the market. Traditional scanning methods are expensive and require more upfront effort. Our unique cloud orchestration architecture scans all entities in a single pass, making it 20x more efficient than other tools. Teams can zoom in on areas they care about, without delays or manual iterations.

Prioritize data stores

Data security teams constantly grapple with the huge number of data stores that they need to protect while realizing that not all data stores are created equal. Using unique DataValuator technology, Normalyze can estimate the cost of breach for each data store helping teams prioritize their security efforts around what matters most. Combined with insights about access and exposure risks, the robust risk matrix allows teams to focus on data stores that carry both a higher likelihood of breach as well as higher financial impact to the organization if breached.

Achieve least privilege access to data stores with ease

By analyzing IAM roles, permissions, database grants and other for user and machine identities Normalyze can quickly identify who has what type of access to a given data store and visualize those insights in Data Access Graphs. By analyzing access logs, Normalyze can conclude who is and who isn't making use of the permissions they have. Security and data teams can quickly determine a large portion of user and machine identities that have permissions to access valuable or sensitive data but don't really need it. By removing those accesses, teams can achieve least privilege access to data and reduce potential attack surface.

Compliance mapping and reporting

Normalyze continuously identifies and highlights data privacy gaps against regulatory compliance benchmarks.

Compliance violations are tagged with both the applicable compliance framework and the individual control that has been violated, so analysts know right away the impact on their compliance posture.

DSPM for AI

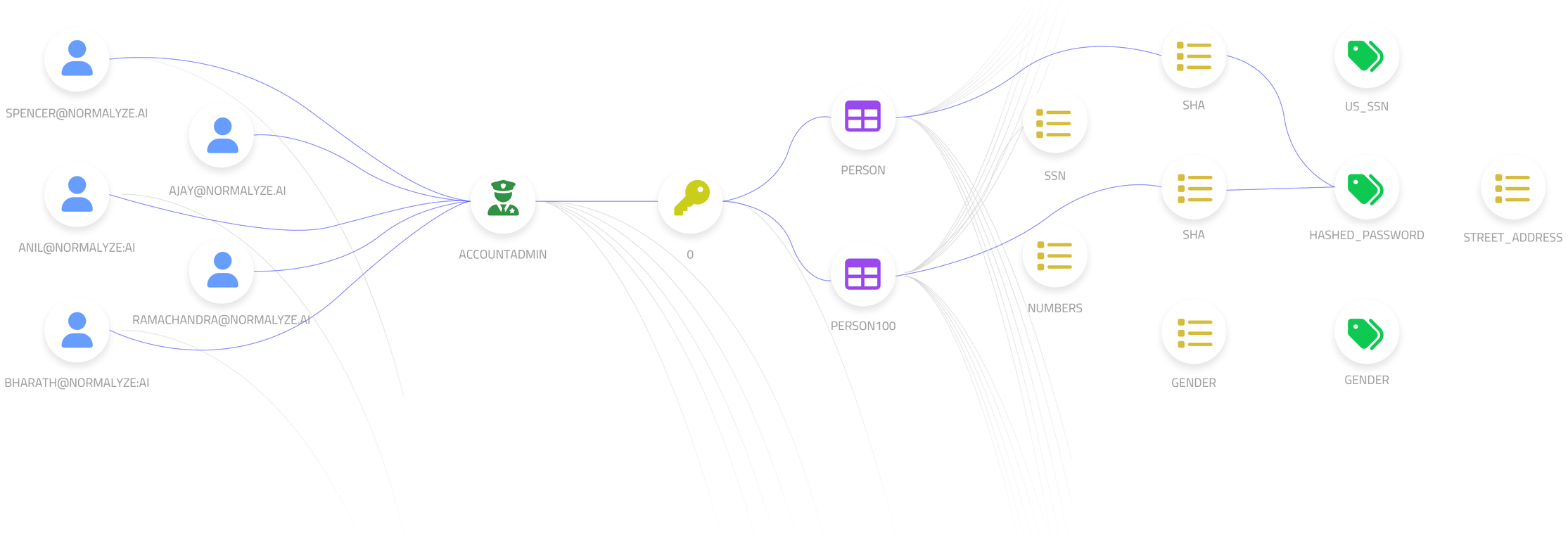
Normalyze scanning also identifies sensitive data being used in Large Language Models (LLMs) like Microsoft Copilot or ChatGPT to ensure that AI-generated content does not expose sensitive company information. In addition, Normalyze helps secure cloud-based AI deployments in AWS Bedrock and Azure OpenAI by detecting any sensitive data being fed into the foundational or custom models.

Normalyze offers specialized APIs for LLM security that can be used to conduct real-time sensitivity analysis of data going into and out of LLMs, providing full governance and visibility into your data usage. These APIs can be easily integrated into existing customer workflows, helping keep costs down and increasing security for services like Microsoft CoPilot.

DSPM for Snowflake

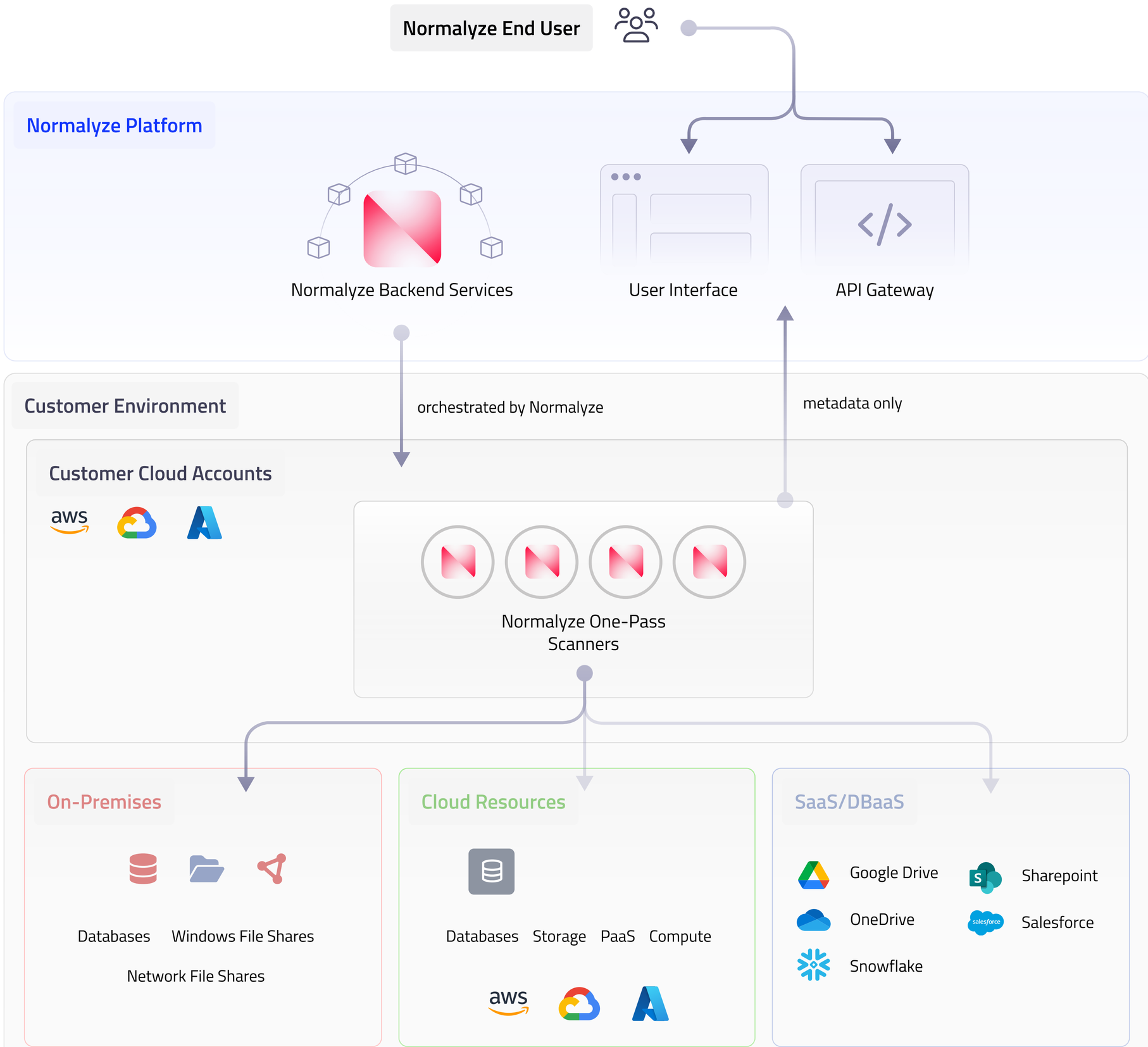
Normalyze offers native integration with the Snowflake Data Cloud, so customers can seamlessly secure their data using Snowflake Horizon's security and compliance capabilities in conjunction with Normalyze's industry-leading data security posture management (DSPM) capabilities to tackle overprivileged access, inefficient or inaccurate data classification, rapid data growth and complexity, data governance challenges and inadequate risk management tools.

Security and data teams can automate continuous data discovery and classification of massive amounts of data, along with precise access management using a customized Data Access Graph, as shown below.



Normalyze Data Access Graph helps teams understand user access privileges to sensitive data within Snowflake at a granular level

Normalyze Architecture



Using the permissions provided during onboarding, the Normalyze platform deploys the single pass scanner cloud functions and VMs within your cloud environment. The spin up, scaleout, scale down and tear down are all managed by the Normalyze platform. The scanners have read-only access to perform these inspections only when they are deployed within your environment. Data within your environment is accessed using a variety of methods including API based access and snapshotting within the environment to recreate datastores. Once scanning is complete, the scanner sends only the relevant metadata back to Normalyze for further processing and then safely terminates. This process, facilitated by scalable cloud-native technologies, ensures that all data-scanning activities are confined to internal resources, thereby preserving the privacy and integrity of your data.

A fundamental advantage of Normalyze's DSPM platform lies in its ability to perform security scans within the native data environment. That means valuable and sensitive data does not need to be moved or copied outside its original location for security analysis, significantly minimizing potential exposure to threats and vulnerabilities that could arise during data transfer. This provides customers with a highly cost-effective approach compared to other data scanning approaches that require either snapshotting or egressing the data to external vendor locations.

By keeping data within its native ecosystem, Normalyze also helps organizations reduce their overall attack surface and streamline compliance efforts.

Supported Platforms and Technologies

Normalyze's data discovery capabilities are engineered to operate seamlessly across a diverse range of platforms and services. By supporting an extensive array of data stores, from traditional relational databases to modern NoSQL and key-value stores, Normalyze ensures comprehensive visibility into all structured, unstructured, and semi-structured data. This integration extends across major cloud providers and SaaS platforms, including but not limited to AWS, Azure, Google Cloud Platform (GCP), and various enterprise applications like Snowflake, Salesforce and Workday.

Normalyze's common data discovery and classification framework enables adding support for new data store technologies quickly. Supported technologies include, but are not limited to:

S3 Buckets, EBS, RDS, Redshift, DocumentDB, MemoryDB. DynamoDB, Keyspaces, Elasticache, EC2 DBs

Buckets, CloudSQL, MemoryStore, BigQuery, BigTable

Blob Store, File Share, SQL Server, MYSQL Server, PostgreSQL Server, Azure Cache, CosmosDB, Synapse Analytics, MariaDB, NetApp Files

Cloud + SaaS Platforms

Snowflake, Google Drive, OneDrive, Sharepoint, Salesforce

On-Premises

Windows File Share, MySQL, Postgres, MSSQL, MongoDB, Oracle DB, Network File Share

Conclusion

The Normalyze DSPM platform offers a transformative approach to data security, addressing the critical needs of today's dynamic IT environments.

Normalyze not only offers a sophisticated technical solution but also facilitates an environment for security and data teams to collaborate on data security action plans.

Let us help secure your data... wherever it is.

See Normalyze in action. Request a demo or take advantage of our Data Risk Assessment to understand how our platform can make a significant difference in managing and securing your organization's most valuable data assets.

Visit **www.normalyze.ai** to get started.

Normalyze®

data-first cloud security