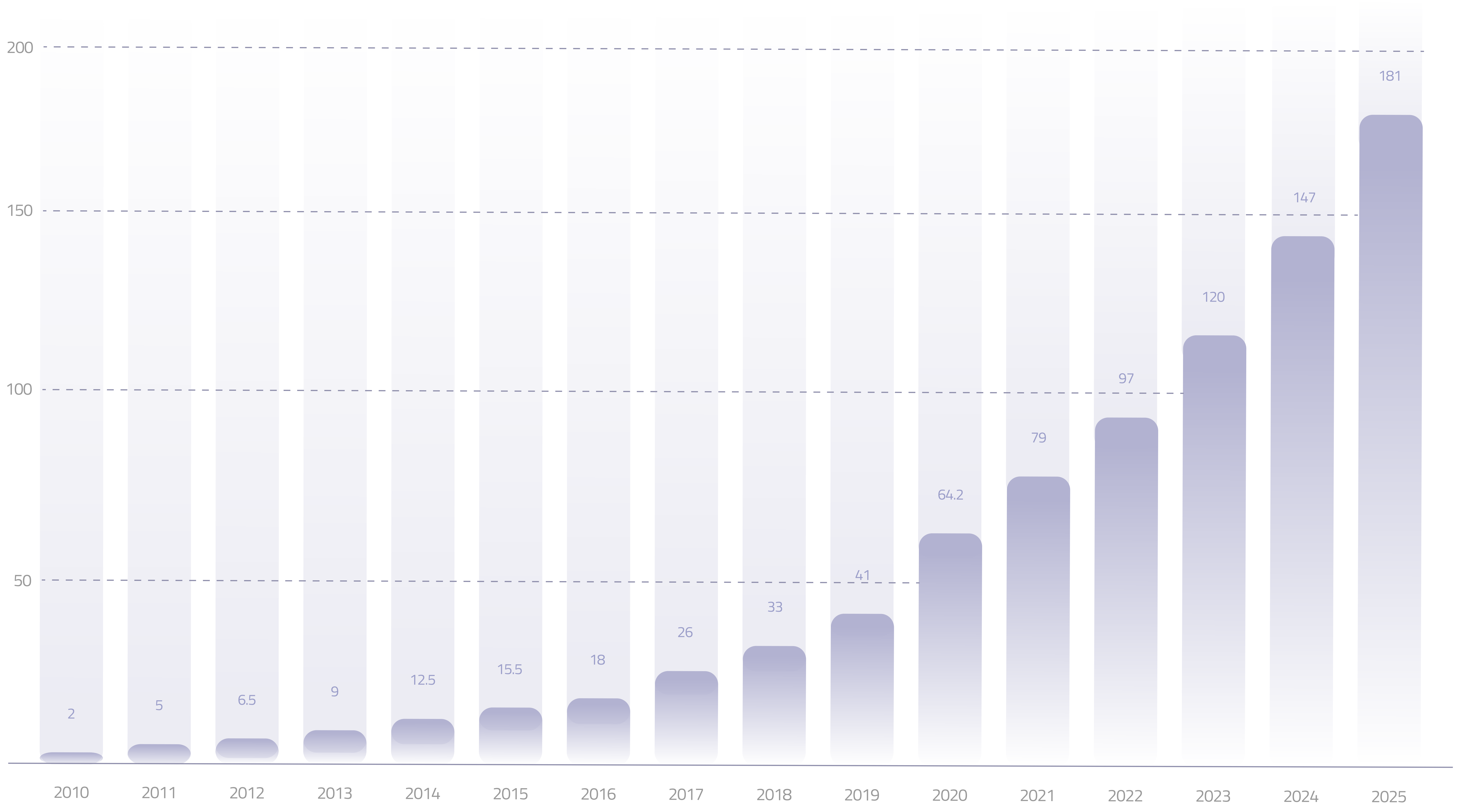
Normalyze™

data-first cloud security

Data-first cloud security for the digital enterprise

Company Backgrounder



Data volume in zettabytes

Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025. (in zettabytes) © Statista 2022.

How Normalyze secures the data within everything you build and run in the cloud

The rise of enterprise cloud computing has brought an even greater emphasis on data. Many analysts and economists refer to today as the "data-driven economy." This is for great reason: after trillions of dollars invested globally into digital transformation efforts, most business interactions today are digital.

And its data that drives artificial intelligence and machine learning investments and improves organizational decision-making. According to data compiled by Statista, two zettabytes of data were created, captured, copied, and consumed globally in 2010. That figure will reach 97 zettabytes this year and 181 zettabytes by 2025.

This data includes everything needed to function in today's economy, from the business. And as companies increasingly run on the cloud, data is becoming increasingly scattered as monolithic application architectures give way to microservices architectures. This microservices proliferation is a catalyst for considerable data proliferation.

There are other catalysts as well. There's an endless hunger for data to feed artificial intelligence/machine learning modeling. There's the amount of data being unleashed within multi-cloud environments and application APIs.
The equation is simple: the more clouds and the more digital transformation, the more data managed and consumed.

The rise of cloud computing has also increased the complexity of the enterprise attack surface. Modern development pipelines deliver continuously, while the move to "infrastructure as code," as well as microservices, makes it all too easy to misconfigure workloads and cloud services as configurations change, identities and their privileges evolve, and data stores become increasingly intricate.

"Data is eating the cloud due to many trends like AI & ML and the move from on-prem environments to IaaS and PaaS. Existing cloud security solutions are falling short to help companies discover, classify sensitive data and secure it. This is the problem Normalyze is set to solve across all public clouds and at scale".

Amer Deeba, CEO and co-founder at Normalyze.

The growing data security and regulatory challenge

The growing complexity of cloud computing is a big part of why breached data records have risen (according to the Identity Theft Resource Center) from 16 million in 2010 to more than 155 million today. A recent survey from IDC found that 98% of organizations they queried reported at least one cloud data breach in the past 18 months.

Finally, there is ever-increasing concern around data governance mandates, privacy regulations, and data breach disclosure laws worldwide. The challenge is that cloud systems and data are so fluid that chief information security officers and security teams have a tremendous challenge securing their highly dynamic multi-cloud environments.

As we detail next, legacy and current security tools do not match the data security challenge.

Current cloud-security tools can't effectively secure enterprise cloud data

As the enterprise adoption of cloud computing continued to evolve, so did how enterprises approached securing their data. Today, enterprises find their data scattered throughout their various cloud systems, and they have lost visibility into where their sensitive data resides. Whether there are any shadow data stores that developers left abandoned? Who can access all of the enterprise data on these clouds, and are there excessive privileges? What data is at risk of being breached and falling out of regulatory compliance?

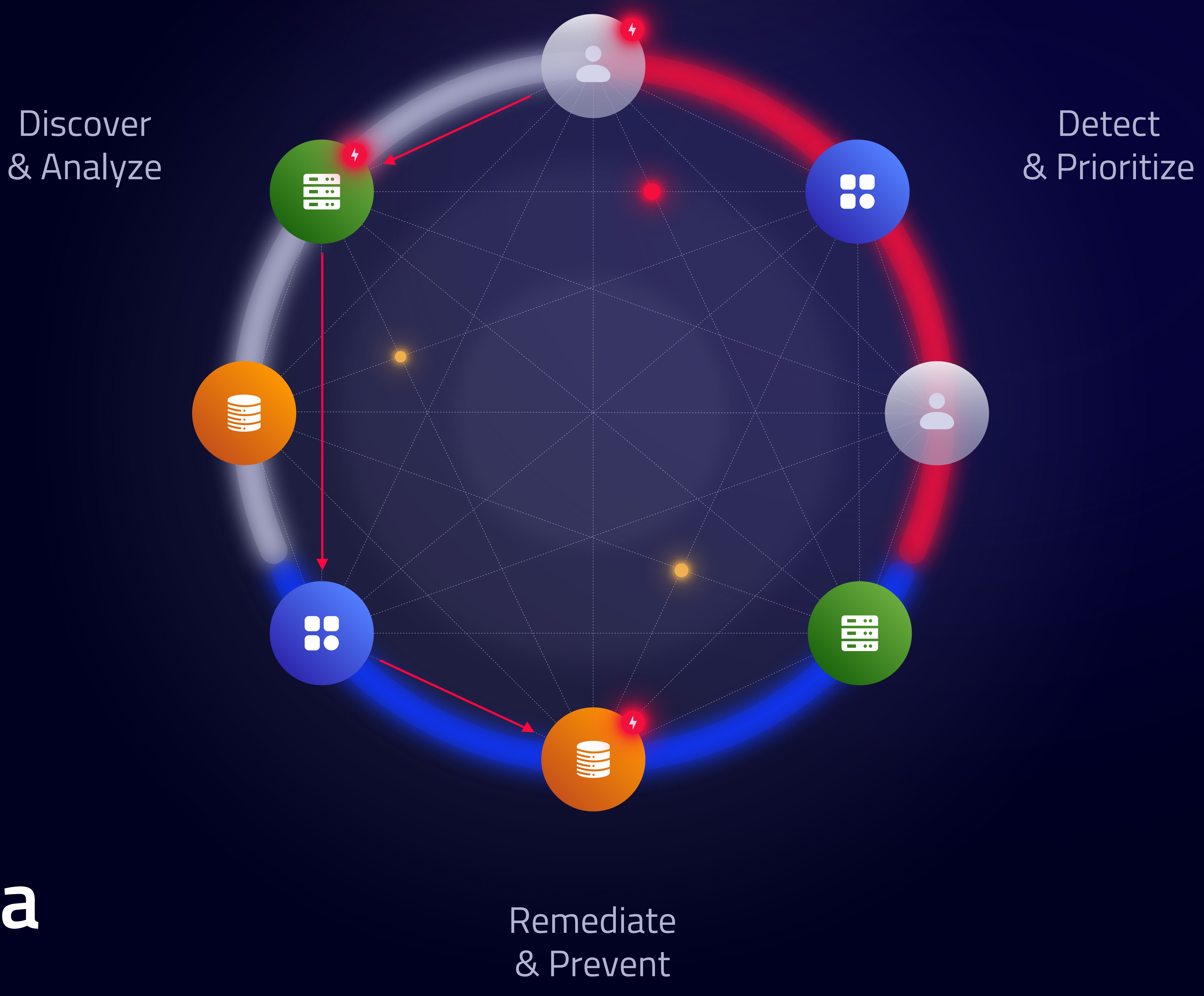
These are essential questions and complex challenges for enterprise security teams. To keep data secure, enterprises need to be able to continuously discover, classify and protect their data. And to do so, enterprises have been working with several security tools, such as data loss and prevention platforms to discover data and attempt to block its leaking, change management databases to track assets and their location, cloud security posture management, and SaaS security posture management programs to try to minimize their attack surface. The difficulty is that each of these tools addresses a particular aspect of the problem or two, and they don't tend to work together effectively, if at all. Enterprises attempt to use these security tools to secure their cloud systems and data. The challenge for each of these tools is that they generate an unmanageable number of alerts, but they all work in silos with no synergy among the various security toolsets. Enterprises need to accurately identify where their (structured and unstructured) data resides in their cloud systems. They need to know what data is sensitive or regulated, who has access (and at what levels of access) to that data, and how the workloads and supporting infrastructure that supports that data may place that data at risk. As they find vulnerabilities, misconfigurations, and incorrect user access levels, they need to prioritize their mitigation plan so that the most pressing risks that lead to sensitive data are fixed first.

This gives CISOs the full context they need to avoid costly data breaches, and rapidly mitigate those that do strike before serious damages occurs.

Data security tools need to work synergistically. This is the set of challenges Normalyze solves. Normalyze will first identify the organization's cloud systems and then discover the most sensitive structured and unstructured data within those systems. Normalyze will determine who has access to that data and their level of access.

Normalyze will also discover the microservices in use and identify their vulnerabilities and misconfigurations that place data at risk. With Normalyze, security teams, CISOs, GRC professionals, and DevOps teams can view their entire cloud infrastructure. They can see in one concise place where their most essential data reside and prioritize the securing of that data based on risk. This way, enterprises always know that their most important data is secured.

In the next section,
we will look how Normalyze achieves this.



How the Normalyze platform improves the security of enterprise cloud data

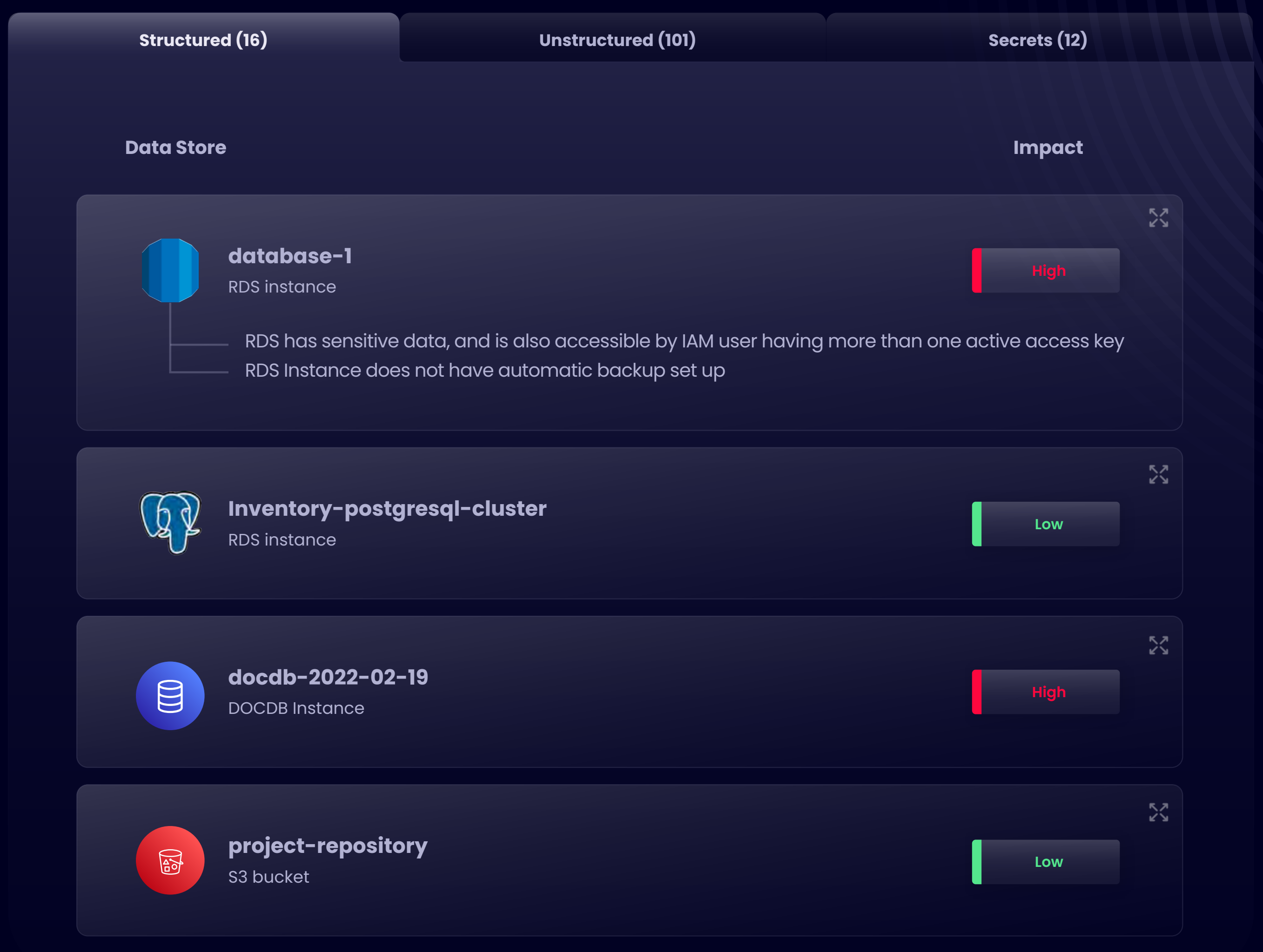
» Through its agentless assessment, data discovery, data classification, AI driven vulnerability analysis, risk prioritization, and comprehensive and actionable remediation insights, Normalyze helps enterprises understand the complete picture when it comes to data risks.

That includes everything needed to be discovered and understood around the applications, infrastructure, configurations, vulnerabilities, and the identities and permissions associated with the user and system access.
Everything is provided within the graph and connects all factors necessary to identify data and correlate risks.

Normalyze Platform

Discover & Analyze

Discover resources, sensitive data, and access paths



Data Store	Impact
database-1 RDS instance RDS has sensitive data, and is also accessible by IAM user having more than one active access key RDS Instance does not have automatic backup set up	High
Inventory-postgresql-cluster RDS instance	Low
docdb-2022-02-19 DOCDB Instance	High
project-repository S3 bucket	Low

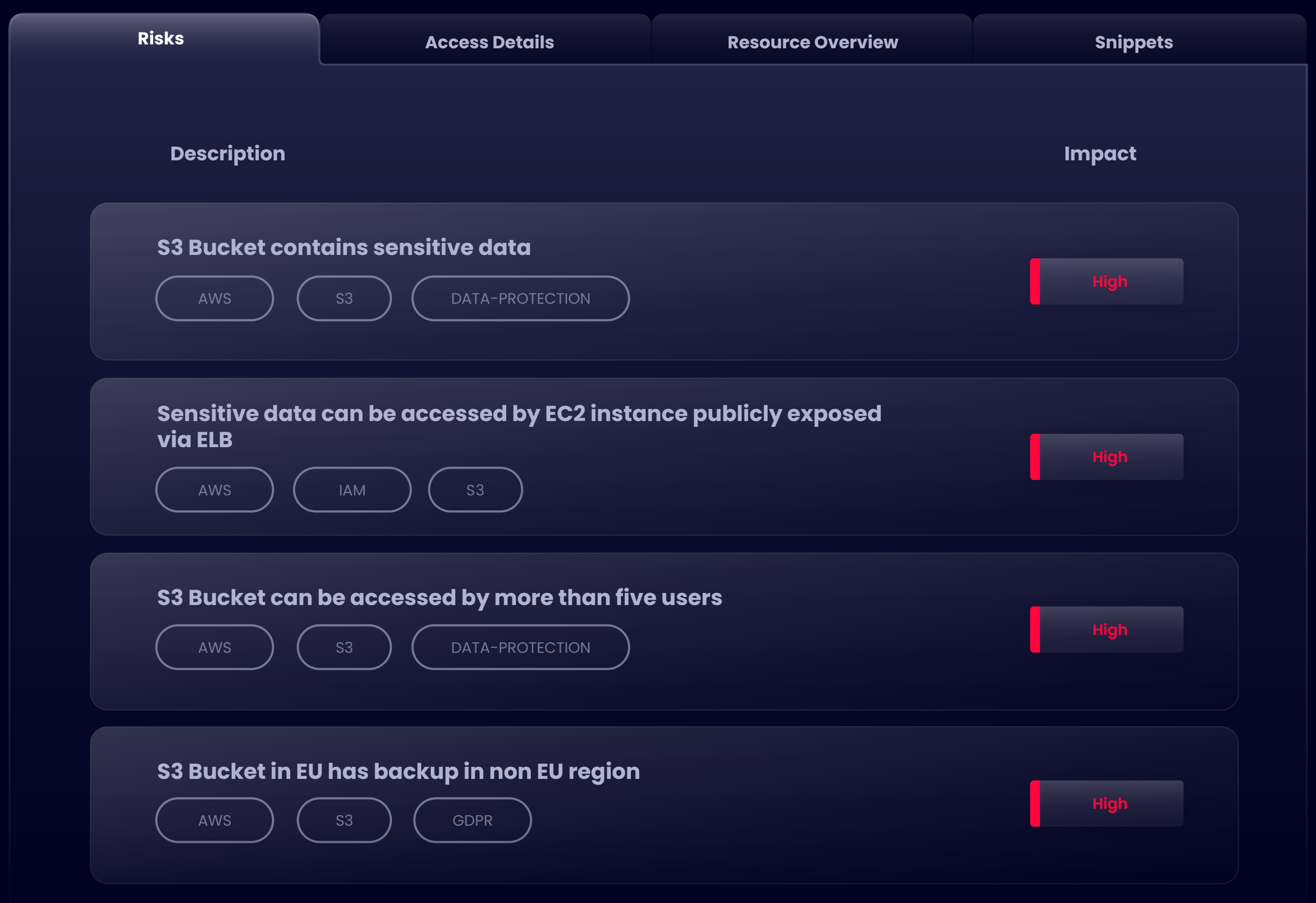
The Normalyze platform initially performs its agentless cloud discovery scan to identify all cloud systems in the environment. During this discovery of cloud resources, Normalyze identifies and prioritizes everything running operationally in the cloud environment. During the Discover and Analyze phase of the assessment, enterprises will understand their cloud environment and interconnected systems.

During the Discover and Analyze phase, Normalyze's AI-backend also scrutinizes all structured and unstructured data within the cloud environment.

During this phase, Normalyze identifies and builds a graph of all available cloud resources; what identities have access to these systems, their permissions, and all of the available data stores. These assessments are completed continuously.

Detect & Prioritize

Track resource configuration, deep context, and transitive trust relations in real-time as a graph



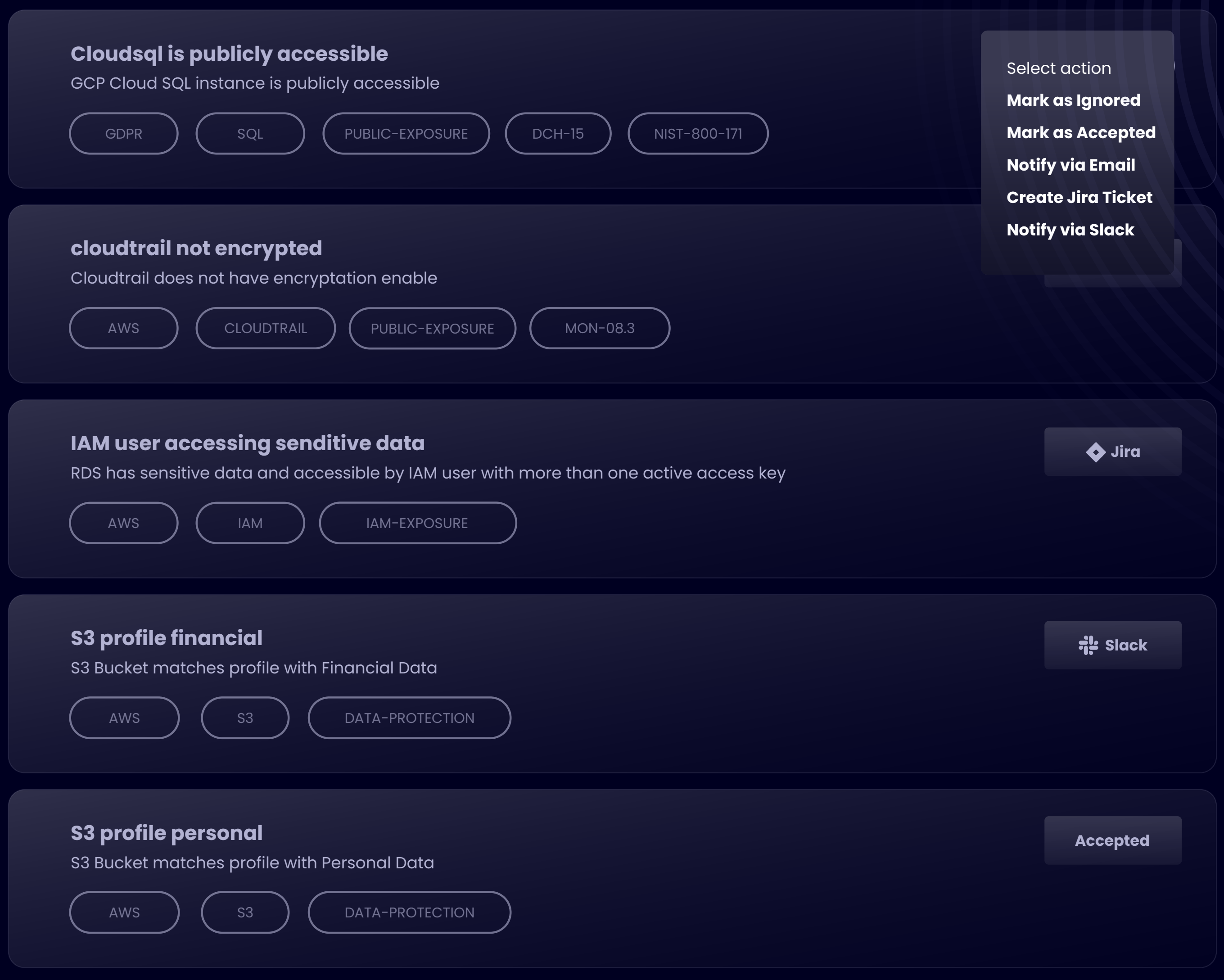
Description	Impact
S3 Bucket contains sensitive data AWS S3 DATA-PROTECTION	High
Sensitive data can be accessed by EC2 instance publicly exposed via ELB AWS IAM S3	High
S3 Bucket can be accessed by more than five users AWS S3 DATA-PROTECTION	High
S3 Bucket in EU has backup in non EU region AWS S3 GDPR	High

Normalyze will then prioritize proprietary, regulated, and otherwise sensitive data and rank it in its importance and risk level. The risks are determined by vulnerability severity, the nature of the data, its access paths, and the condition of its resource configurations.

The agentless Normalyze assessments are continuous. Every time an asset is added, changed, or removed, the graph is instantly updated. In this analysis, the identity and permission information is considered, along with uncovered vulnerabilities and misconfigurations that could lead to a data breach. The AI-driven analysis will look at everything within the cloud environment and identify all of the possible paths to sensitive data and potentially viable attack vectors. As access, systems, and configurations change, new risks that can't be swiftly mitigated can be introduced.

Further, all of the discovered data, whether structured or unstructured, is prioritized based on sensitivity and associated regulatory controls, whether PCI DSS, HIPAA, or GDPR. Normalyze will highlight the data that needs immediate attention. The Normalyze one-pass data scanner samples enterprise data to detect sensitive entries (names, social security numbers, credit card numbers, street addresses, email addresses, and so such) within data stores. addresses, email addresses, and so such) within data stores. Normalyze then connects the data via specific profiles to confirm the presence of Personally Identifiable

Information, payment card data, Health Insurance Portability and Accountability Act, or other sensitive and proprietary data. This is a unique feature to the Normlayze data scanner that helps customers reduce false-positives and increase efficiency of scans, Importantly, none of this data ever leaves the control of the customer or ever moves to another cloud, nor is it ever transferred to another region or nation. The only data that leaves is the information Normalyze collects about the data, or the metadata, necessary to create the graph.


Cloudsql is publicly accessible
GCP Cloud SQL instance is publicly accessible

cloudtrail not encrypted
Cloudtrail does not have encryptation enable

IAM user accessing senditive data
RDS has sensitive data and accessible by IAM user with more than one active access key

S3 profile financial
S3 Bucket matches profile with Financial Data

S3 profile personal
S3 Bucket matches profile with Personal Data

Remediate & Prevent

Visualize, analyze, and automate actions

With cloud assets discovered, data identified and classified, and then remediation prioritized based on sensitivity, enterprise security teams are ready to take steps to remedy the most pressing data risks and work down from there.

After the assessment, security analysts and others can also query the graph to see where specific risks exist. For instance, they can search for every Amazon EC2 instance with a role that can read an Amazon S3 bucket with a specific file type, such as one containing personally identifiable information. Or, the analyst can search the graph for any software running a pressing vulnerability, such as Log4j, that may directly or indirectly expose sensitive data to the internet. For recurring instances, teams can create alerts for certain conditions that may require mitigating.

As Normalyze identifies risky conditions, its prioritization engine makes all of the conditions that place data at risk so that teams understand what steps they need to remedy the situation. Remediation efforts can be dispatched to a service management platform, or other automated measures can be taken. Specific groups or individuals can be alerted to remedy the vulnerability, or steps can be taken to remove access.

Detail use cases: CISO, Security engineer, GRC, DevOps

Normalyze provides rapid time to value. Typically, enterprises will deploy Normalyze to their cloud environment within 30 to 45 minutes. And they then conduct their first discovery and sensitive data assessments and their first graph within 15 minutes.

The Normalyze Platform provides value to all security stakeholders:

- **Chief Information Security Officer**
  Always up-to-date security posture
  Proactively prioritize recommendations to improve data security posture
- **Security Enginner**
  Prioritized Risks
  Track issue recurrence over time
- **Goverananance, Risk Managenemt, Compliance**
  Discover sensitive data and any compliance gaps with drill-down capabilities for data officers
- **DevOps**
  See entire operational, infrastructure, and development pipeline for security visibility

"We've built Normalyze from the grounds up with a frictionless deployment model so customers can deploy it fast and get the value they are looking for to discover all their cloud data stores and identify attack paths that can lead to sensitive information. We are the only platform that is combining data with identity, access, configs and vulnerabilities to give customers a holistic view about their cloud data security posture and help them orchestrate remediation efforts across all three clouds".

Ravi Ithal, CTO and Cofounder at Normalyze.

Data-first cloud security

Conclusion

The rise of enterprise cloud computing has indeed brought an even greater emphasis on data. And it's brought tremendous change to enterprise data security, as well. Normalyze, through its agentless assessment, data discovery, AI-driven vulnerability analysis, risk prioritization, and comprehensive and actionable remediation insights, helps enterprises understand the full range of risks present against their data.

That includes everything needed to be discovered and understood surrounding the cloudapplications, infrastructure, configurations, vulnerabilities, and the identities and permissions associated with access. Everything is provided within the graph and connects all factors necessary to identify data and correlate risks. This enables enterprises to discover, visualize, and secure their cloud data. To learn more about how you can secure your enterprise data within minutes and sign up for your free account, visit www.normalyze.com today.

Normalyze™

data-first cloud security

Contact

Amer Deeba
Co-Founder

amer@normalyze.com
(408) 757 2456

normalyze.com