CYERA

REPORT

Top 5 Findings from Cyera Data Risk Assessments

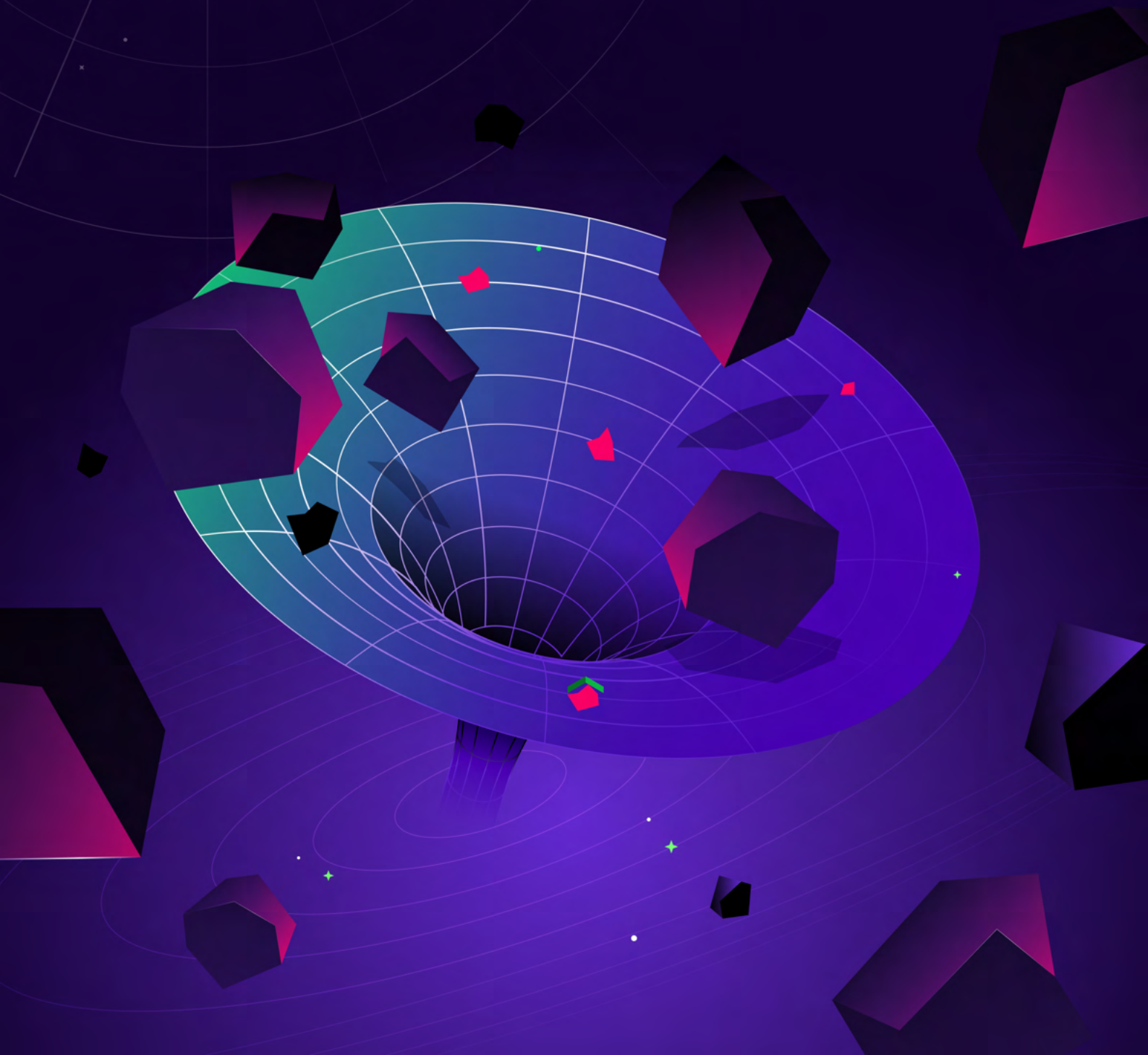


Table of Contents

Executive Summary

Data is your business. But do you know how exposed it is?

As data grows and AI-driven attacks evolve, traditional data security falls short. Business leaders need to answer hard questions: Where is our sensitive data? Who can access it? Is it truly protected?

Cyera's Data Risk Assessments uncover what other tools miss. In this report, we break down the five most critical data security risks found across enterprises - and how smart teams are closing the gaps. These are real-world vulnerabilities with real-world consequences: breaches, compliance violations, and business disruption.

Get the visibility you need to protect your most valuable asset - your data.

Why Consider a Data Risk Assessment?

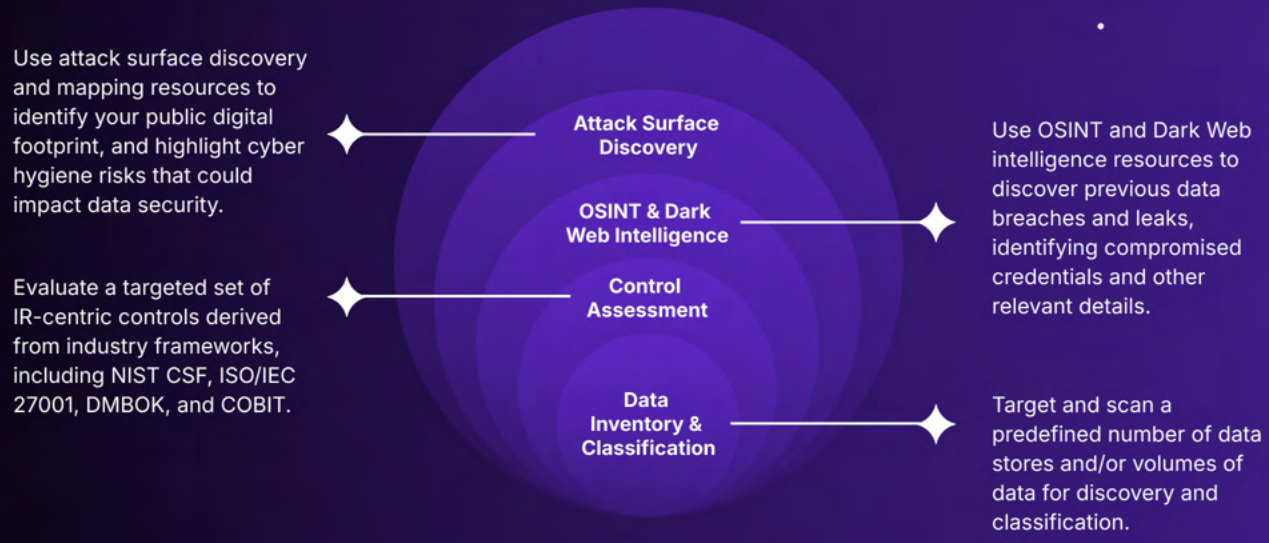
Despite billions invested in cybersecurity, most organizations still lack clarity into their true data security posture.

A Cyera Data Risk Assessment (DRA) helps security and data leaders:

- Identify high-impact data risks others miss
- Validate and improve internal controls
- Demonstrate compliance and governance maturity

Whether you're reporting to the board or preparing for an audit, a DRA delivers the insights you need - fast

Cyera's Risk Assessment Methodology



What a Data Risk Assessment Can Do for You

A Data Risk Assessment powered by Cyera gives you:

- **Real-time visibility** into where your sensitive data lives and who has access to it.
- **AI-driven risk prioritization** that focus on the risks that matter most.
- **Automated remediation guidance** for faster risk reduction.
- **Regulatory alignment** to ensure compliance with PIPEDA, GDPR, HIPAA, PCI DSS, CCPA, and more.

See what you've been missing. Request a Data Risk Assessment today.

Critical Findings

These are the five most critical data security risks facing organizations today:

01	Credentials Stored in Plain Text
02	Unauthorized External Access to Sensitive Data
03	Ghost Datastores Containing Sensitive Data
04	Credit Card Numbers in Plain Text
05	Public/External Data Exposure

01 Credentials Stored in Plain Text

Description

Authentication data is extremely sensitive, and should never be stored in plain text, even if disk encryption is applied. PCI DSS requirement 8.2.1 demands using encryption to render all authentication credentials (such as passwords, access tokens, and phrases) unreadable during storage on all system components.

Data Classes Found

Password

Datastore

aws canada-employees

Data Contexts Found

Identifiable

Affected Records

9.9K

CRITICAL

Finding

Sensitive authentication credentials (passwords, API keys, and tokens) were discovered in plaintext across cloud platforms in:

- Configuration files
- Scripts
- Documentation
- Public repositories

This exposure enables anyone with file access to infiltrate internal systems and compromise data.

Business Risk

Unencrypted credentials create immediate risk, allowing attackers to:

- Access critical systems
- Exfiltrate data through compromised accounts
- Trigger compliance violations with financial and reputational consequences

Impact: 9.3 billion records at risk, highlighting a systemic issue with credential exposure.

How Cyera Helped

Cyera's AI engine detected and prioritized at-risk credentials while identifying patterns in secrets management practices. This enabled automated detection and stronger security policies to be implemented.

- **Tactical:** Remove exposed credentials, rotate compromised keys, and enforce access controls.
- **Strategic:** Strengthen secrets management through automation, encryption policies, and development workflow integration.

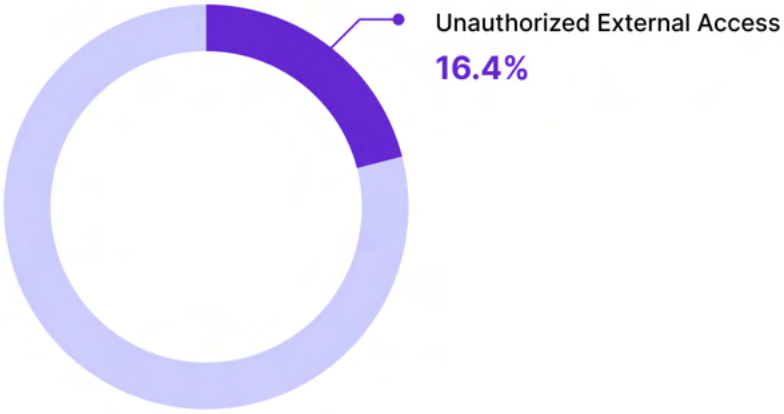
Cyera's Advantage

AI-native scanning ensures comprehensive detection of exposed credentials across all formats, preventing breaches and eliminating this highly exploitable security risk.

02 Unauthorized External Access to Sensitive Data

21.2B | 16.4%

21.2B / 129.3T Sensitive Records at High Risk



Finding

Unauthorized external access to sensitive corporate data was detected, including former contractors, vendors, and partners retaining access beyond their need. This excessive access leaves critical data vulnerable to misuse and compliance violations.

Business Risk

Unauthorized external access significantly increases the risk of:

- Data breach likelihood from external users exfiltrating or leaking data
- Regulatory violations with CCPA, PIPEDA, GDPR, HIPAA and PCI DSS
- Supply chain threats from former contractors inadvertently exposing data

Impact: 21.2 billion records at risk - a persistent oversight in access governance and entitlement review.

How Cyera Helped

Cyera provided full visibility into external access patterns, identifying high-risk permissions and unauthorized sharing. By mapping data flows and access rights, security teams could rapidly remediate risks and enforce stronger governance.

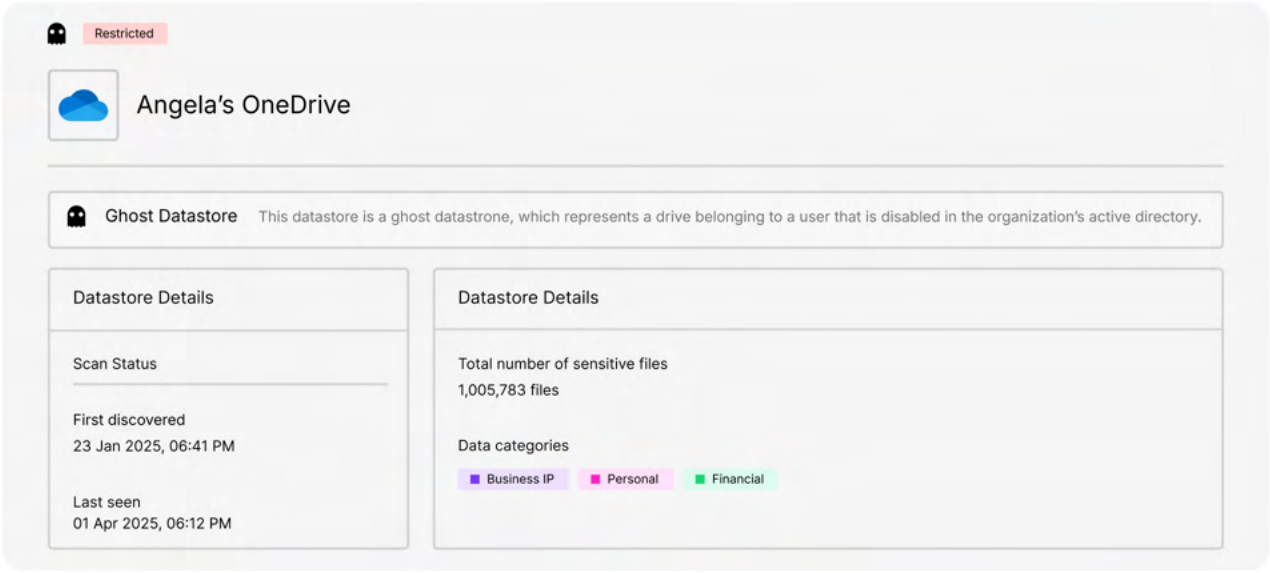
Tactical: Revoke unnecessary access, implement least privilege controls, and enable continuous monitoring.

Strategic: Automate access reviews, enforce policy-based controls, and align with global compliance frameworks.

Cyera's Advantage

Real-time monitoring and risk scoring identify and eliminate unauthorized access - protecting data before it becomes a breach risk.

03 Ghost Datastores Containing Sensitive Data



Finding

"Ghost datastores" – inactive or forgotten data repositories containing sensitive information – were discovered outside active security controls. These unmonitored assets include:

- Decommissioned databases
- Old storage buckets
- Snapshots
- Abandoned development environments with production data

Business Risk

Ghost datastores introduce:

- Data breach risks from unsecured assets being exploited
- Regulatory violations from uncontrolled retention of sensitive data
- A larger attack surface and unnecessary storage costs

Impact: Ghost datastores are among the most overlooked risks - exposing vast amounts of data.

How Cyera Helped

Cyera identified and mapped ghost datastores across cloud platforms, providing comprehensive visibility and enabling automated cleanup workflows.

Tactical: Identify datastores, enforce retention policies, encrypt/remove outdated data.

Strategic: Establish data lifecycle management, integrate discovery into security programs.

Cyera's Advantage

AI-native classification identifies sensitive data within ghost datastores – even with missing metadata – ensuring complete discovery and risk elimination.

04 Credit Card Numbers In Plain Text

Is It At Risk?

POLICY	ISSUES	SEVERITY	DATASTORE
Encryption Unencrypted credit card numbers in ghost data store	14 issues	CRITICAL	Azure SQL Database
Data Dispersion Financial data outside of user defined Financial Zone'	4 issues	CRITICAL	Azure Storage Container
Public Exposure Sensitive files are publicly exposed in Azure Blob Storage	1 issue	CRITICAL	Azure Storage Container

Finding

Unencrypted credit card numbers were found in:

- Databases
- Document repositories
- Communication platforms

Typically the result of coping payment data to test environments or storing in customer service logs without encryption.

Business Risk

Unencrypted credit card data creates immediate business exposure:

- Regulatory violations with PCI DSS, GDPR, PIPEDA, and CCPA
- Fraud-related losses and erosion of customer trust
- Legal liability for non-compliance with payment industry requirements

Impact: 73.1 billion records at risk from exposed credit card data - driving significant financial and regulatory exposure.

How Cyera Helped

Cyera's AI engine identifies exposed credit card numbers using advanced pattern matching, enabling PCI-compliant encryption and tokenization.

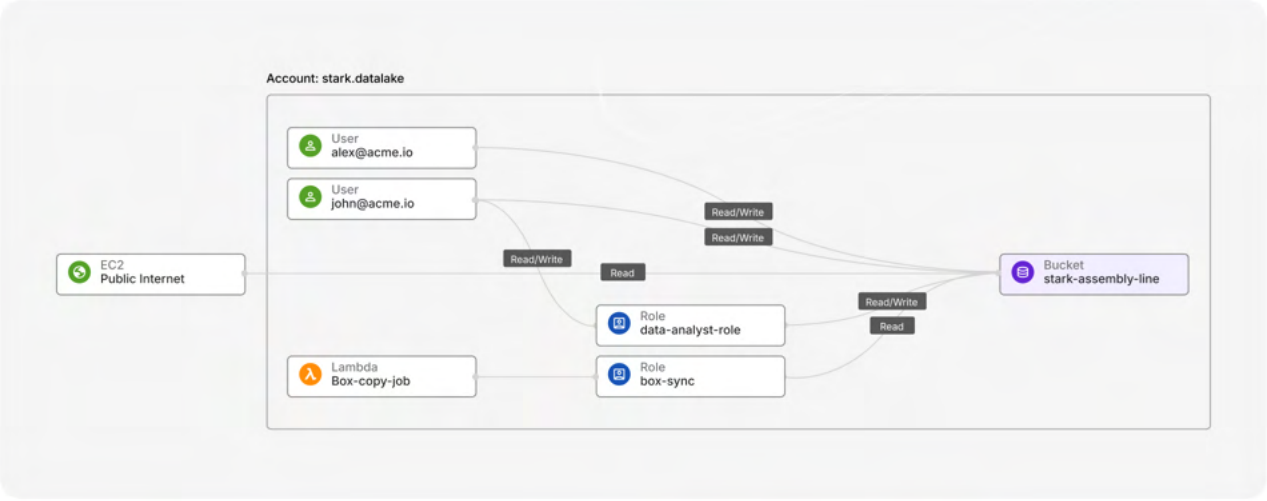
Tactical: Remove plaintext card data, implement tokenization, and enforce data masking.

Strategic: Automate payment data protection while ensuring regulatory compliance.

Cyera's Advantage

Context-aware scanning detects exposed payment data accurately, reducing false positives and ensuring compliance enforcement at scale.

05 Public Data Exposure



Finding

Sensitive data was frequently exposed through misconfigured access controls, making records publicly accessible without authentication. Primary causes included publicly accessible cloud storage, overly permissive sharing settings, and improperly secured APIs.

Business Risk

Public exposure creates immediate security risks requiring no sophisticated attacks to exploit:

- Mass data breaches from easily discoverable exposed records
- Regulatory violations leading to fines and reputational damage
- Exploitation by cybercriminals for fraud and identity theft

Impact: Billions of records publicly exposed - a misconfiguration issue that's both avoidable yet alarmingly common.

How Cyera Helped

Cyera continuously monitored for public exposure, providing real-time alerts on misconfigured access. By analyzing exposure patterns, organizations could enforce proper access governance and implement automated compliance checks.

- **Tactical:** Remediate exposed data, enforce least privilege, secure APIs, implement monitoring.
- **Strategic:** Strengthen access governance through automated compliance checks and policy enforcement.

Cyera's Advantage

Risk-based prioritization enables rapid remediation of critical vulnerabilities, while machine learning predicts potential misconfigurations before they occur.

The Cyera Advantage

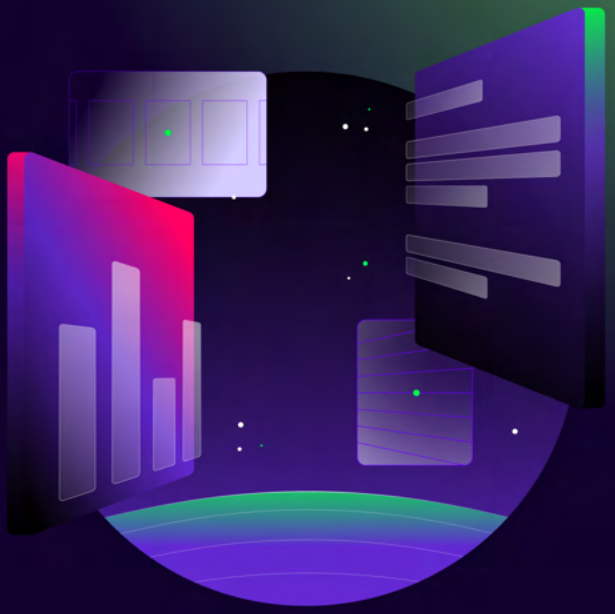
Data security should enable innovation - not slow it down.

Cyera's AI-native platform delivers unmatched speed and scale. It scans billions of records in near real time with 99.9% precision - without performance impact.

Our adaptive machine learning eliminates false positives and flags emerging threats before they surface. By continuously analyzing data patterns and access behaviors, Cyera helps you identify and fix security gaps before they become incidents.

And with an agentless architecture and deep contextual intelligence, Cyera connects your data to your business — transforming security from a technical hurdle into a strategic advantage.

Assess Your Data Risk - Fast



Gain instant visibility into your data risk and compliance posture - with minimal lift from your team.

Cyera's Data Risk Asessments combine AI-powered analysis with targeted stakeholder interviews to deliver maximum insight. You'll receive:

- A prioritized view of key risks
- A clear, security improvement roadmap
- A fast, zero-friction setup

GET STARTED WITH A DATA RISK ASSESSMENT TODAY

VISIT CYERA.COM/DRA TO SCHEDULE A 30-MINUTE CONSULTATION WITH OUR EXPERTS — NO SETUP REQUIRED.

Trusted by

AT&T · docusign · Paramount · newamerican FUNDING · LifeLabs · CHIPOTLE · advance · SKECHERS · UiPath · FINANCE of AMERICA · PELOTON · Cboe