Optimization suggestions:

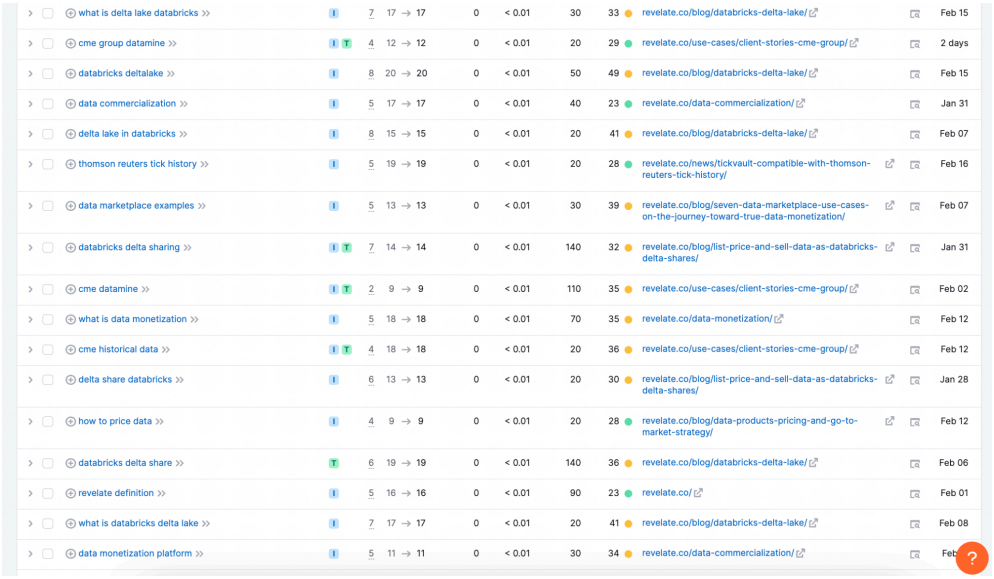
- This article is way too technical. Search intent-wise, this site ranks for all of the top keywords Relevate wants to rank for an should be our North Star.
    - Based on this, it's clear that **readers want to get to the point**. They don't want a run down on "what is involved, what are the types etc"
    - So, I think we should cut all of the unnecessary sections like "what is involved in securing cloud data?" "types of access control" etc. Also delete all of these data privacy laws sections. You can add a callout box to them maybe with just a single line on what each one is but that's it.
- On average, the top articles have only 1.3k words so we need to trim.
- I also suggest changing the button or CTA color. It blends in with the rest of the site. I propose changing the button color to purple or orange or some color that can pop from the green. Or change the CTA's background to the purple color of their logo.
- Also, make sure every image in the article is saved under a file name using variations on the keyword. This would be up to the client (Relevate) to make sure of.
- I like to add a related articles section linking out to three related articles at the bottom of the article.

Proposed outline:

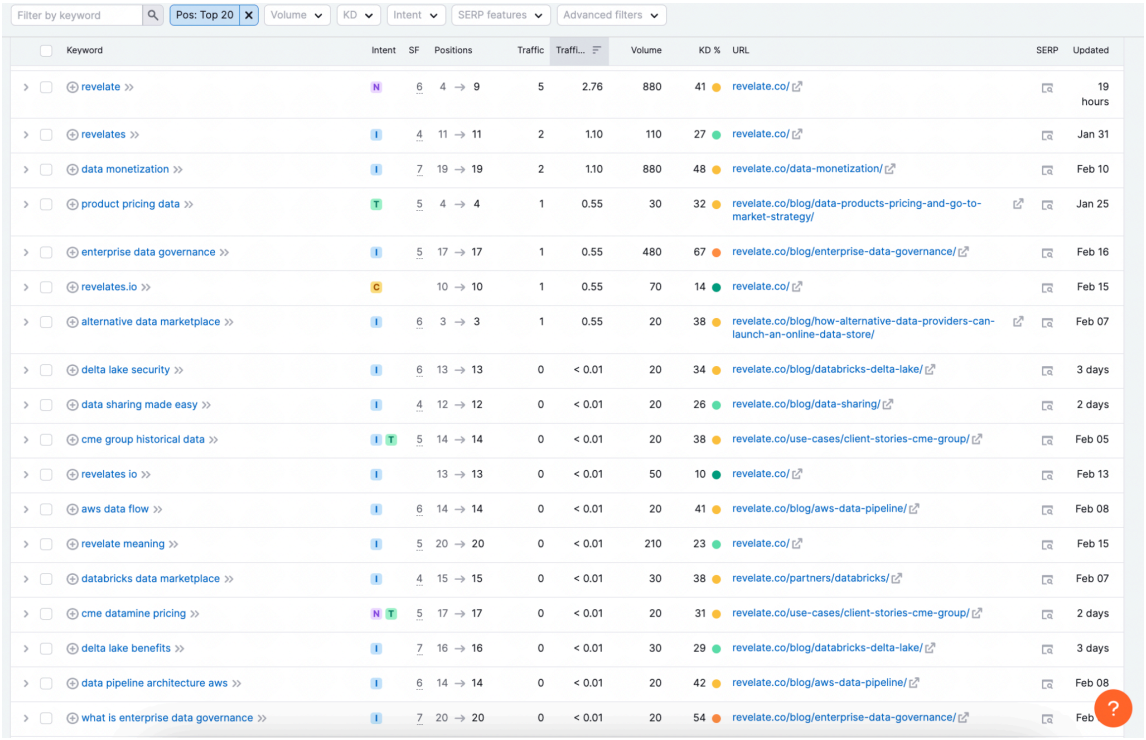
- **Introduction [H2]**
- **What is cloud data security? [H2]**
    - **How secure is the cloud [H3]**
    - Maybe add in an expert tip
- **CTA - IMPORTANT**: make sure the CTA talks about secure data in the cloud instead of the generic one they have.
- **How to secure information in the cloud [H2]**
    - **Using HTTPS or TLS encrypted connections when connecting to cloud storage services [H3]**
    - **Requiring multi-factor authentication (MFA) for any users attempting to access the platform [H3]**
    - **Running regular security tests on cloud data systems to ensure their integrity. [H3]**
- **CTA - MAKE SURE THIS CTA USES DIFFERENT LANGUAGE FROM THE FIRST**
    - **Encrypting all data before uploading it into secure cloud storage spaces [H3]**

    - **Implementing secure server connections for data sharing to reduce third-party intervention during data transmission [H3]**
    - **Setting strict access controls that limit who can view, use, and manage data [H3]**
- **Conclusion**
- **CTA**

Top 20 Keywords:



what is delta lake databricks	I	7	17 → 17	0	< 0.01	30	33	revelate.co/blog/databricks-delta-lake/	Feb 15
cme group datamine	I T	4	12 → 12	0	< 0.01	20	29	revelate.co/use-cases/client-stories-cme-group/	2 days
databricks deltalake	I	8	20 → 20	0	< 0.01	50	49	revelate.co/blog/databricks-delta-lake/	Feb 15
data commercialization	I	5	17 → 17	0	< 0.01	40	23	revelate.co/data-commercialization/	Jan 31
delta lake in databricks	I	8	15 → 15	0	< 0.01	20	41	revelate.co/blog/databricks-delta-lake/	Feb 07
thomson reuters tick history	I	5	19 → 19	0	< 0.01	20	28	revelate.co/news/tickvault-compatible-with-thomson-reuters-tick-history/	Feb 16
data marketplace examples	I	5	13 → 13	0	< 0.01	30	39	revelate.co/blog/seven-data-marketplace-use-cases-on-the-journey-toward-true-data-monetization/	Feb 07
databricks delta sharing	I T	7	14 → 14	0	< 0.01	140	32	revelate.co/blog/list-price-and-sell-data-as-databricks-delta-shares/	Jan 31
cme datamine	I T	2	9 → 9	0	< 0.01	110	35	revelate.co/use-cases/client-stories-cme-group/	Feb 02
what is data monetization	I	5	18 → 18	0	< 0.01	70	35	revelate.co/data-monetization/	Feb 12
cme historical data	I T	4	18 → 18	0	< 0.01	20	36	revelate.co/use-cases/client-stories-cme-group/	Feb 12
delta share databricks	I	6	13 → 13	0	< 0.01	20	30	revelate.co/blog/list-price-and-sell-data-as-databricks-delta-shares/	Jan 28
how to price data	I	4	9 → 9	0	< 0.01	20	28	revelate.co/blog/data-products-pricing-and-go-to-market-strategy/	Feb 12
databricks delta share	T	6	19 → 19	0	< 0.01	140	36	revelate.co/blog/databricks-delta-lake/	Feb 06
revelate definition	I	5	16 → 16	0	< 0.01	90	23	revelate.co/	Feb 01
what is databricks delta lake	I	7	17 → 17	0	< 0.01	20	41	revelate.co/blog/databricks-delta-lake/	Feb 08
data monetization platform	I	5	11 → 11	0	< 0.01	30	34	revelate.co/data-commercialization/	Feb



Filter by keyword | Pos: Top 20 | Volume | KD | Intent | SERP features | Advanced filters

Keyword	Intent	SF	Positions	Traffic	Traffi...	Volume	KD %	URL	SERP	Updated
revelate	N	6	4 → 9	5	2.76	880	41	revelate.co/		19 hours
revelates	I	4	11 → 11	2	1.10	110	27	revelate.co/		Jan 31
data monetization	I	7	19 → 19	2	1.10	880	48	revelate.co/data-monetization/		Feb 10
product pricing data	T	5	4 → 4	1	0.55	30	32	revelate.co/blog/data-products-pricing-and-go-to-market-strategy/		Jan 25
enterprise data governance	I	5	17 → 17	1	0.55	480	67	revelate.co/blog/enterprise-data-governance/		Feb 16
revelates.io	C		10 → 10	1	0.55	70	14	revelate.co/		Feb 15
alternative data marketplace	I	6	3 → 3	1	0.55	20	38	revelate.co/blog/how-alternative-data-providers-can-launch-an-online-data-store/		Feb 07
delta lake security	I	6	13 → 13	0	< 0.01	20	34	revelate.co/blog/databricks-delta-lake/		3 days
data sharing made easy	I	4	12 → 12	0	< 0.01	20	26	revelate.co/blog/data-sharing/		2 days
cme group historical data	I T	5	14 → 14	0	< 0.01	20	38	revelate.co/use-cases/client-stories-cme-group/		Feb 05
revelates io	I		13 → 13	0	< 0.01	50	10	revelate.co/		Feb 13
aws data flow	I	6	14 → 14	0	< 0.01	20	41	revelate.co/blog/aws-data-pipeline/		Feb 08
revelate meaning	I	5	20 → 20	0	< 0.01	210	23	revelate.co/		Feb 15
databricks data marketplace	I	4	15 → 15	0	< 0.01	30	38	revelate.co/partners/databricks/		Feb 07
cme datamine pricing	N T	5	17 → 17	0	< 0.01	20	31	revelate.co/use-cases/client-stories-cme-group/		2 days
delta lake benefits	I	7	16 → 16	0	< 0.01	30	29	revelate.co/blog/databricks-delta-lake/		3 days
data pipeline architecture aws	I	6	14 → 14	0	< 0.01	20	42	revelate.co/blog/aws-data-pipeline/		Feb 08
what is enterprise data governance	I	7	20 → 20	0	< 0.01	20	54	revelate.co/blog/enterprise-data-governance/		Feb

Rewrite Draft

H1: Securing Data in the Cloud: 3 Ways to Protect Your Data

By 2025, over 50% of the world's data will be stored in the cloud, exceeding 200 *zettabytes* of information. This exponential increase in data and storage brings a daily increase in data breaches and security threats. Securing big data in the cloud has never been more critical worldwide for organizations—and their customers.

In 2022, the average cost of a data breach skyrocketed to $4.35 million for U.S. companies. The negative impacts of failing to focus on data security in the cloud are getting far too high for most companies to bear.

Good news: You can quickly and affordably secure data in the cloud through the correct methods, tools, and internal processes.

- What is data security in the cloud?
- Is data secure in the cloud?
- How to secure data in the cloud

H2: What is data security in the cloud?

Cloud computing involves storing data and applications on servers owned and managed by third-party cloud service providers. Data security in the cloud refers to practices around protecting data stored in the cloud and preventing unauthorized access, theft, corruption, or data loss.

H2: Is data secure in the cloud?

Whether data is secure in the cloud depends on various factors, including security measures put in place by the cloud service provider, the individual user's security practices, and the infrastructure of the cloud service platform.

There may need to be more than enabling every possible cloud security measure to secure cloud-hosted data completely. Persisting vulnerabilities include user error (e.g., weak passwords) or misconfigured access controls (e.g., fat-fingered configs). Sophisticated security platforms that can anticipate and resolve real-time security issues are critical solutions when protecting against manual user error and malicious attacks.

Organizations and enterprises can quickly implement proper security measures like data encryption to increase the security of cloud environments and minimize user error vulnerabilities.

H2: How to secure data in the cloud

There are several steps to secure cloud data: using trusted providers, encrypted connections, creating regular backups, and setting least-privileged access controls. These methods help limit unauthorized access to cloud systems and prevent the spread of sensitive information.

A few of the most common methods for securing data in cloud computing include:

- Using HTTPS or TLS encrypted connections to cloud storage services
- Requiring multi-factor authentication (MFA) for users accessing the platform
- Running regular security tests on cloud data systems to ensure the integrity
- Encrypting data before uploading it to the secure cloud
- Implementing secure server connections for data sharing

H3: Using HTTPS or TLS encrypted connections to cloud storage services

Allowing users to use encrypted connections, like HTTPS or TLS, when connecting to your public cloud service platform will help keep data secure and prevent breaches.

To enable encrypted connections for users syncing with your cloud service platform, take the following steps:

1. Obtain a valid SSL/TLS certificate from a trusted Certificate Authority (CA).
2. Configure SSL/TLS on your server by installing your certificate on the server and server software.
3. Redirect HTTP requests to HTTPS to encrypt all traffic.
4. Set up secure communication protocols, like TLS 1.2 or TLS 1.3 to ensure data is transmitted securely.
5. Implement HSTS (HTTP Strict Transport Security) so all subsequent user requests are automatically directed to HTTPS.
6. Test and verify the SSL/TLS connection to ensure it works properly.

H3: Requiring multi-factor authentication (MFA) for users

Requiring multi-factor authentication (MFA, or two-factor authentication) is a top priority for protecting cloud data. With MFA in place, anyone who signs into your platform will need another set of credentials in addition to their password, such as a generated code.

The second level of authentication may come from a second device, like an email, text message, code generator app on a mobile device, or security questions to answer during the sign-in process.

Common multi-factor authentication methods include answering a security question, providing an individual PIN, or inputting a code the provider emails or texts the account holder.

H3: Running regular security tests on cloud data systems to ensure the integrity

Cloud service providers should run regular security tests to ensure the integrity of their data and services. Security testing for protecting data in the cloud can include:

- Vulnerability scanning: These scans can identify potential security weaknesses and can be conducted by automated tools that probe the data center, network, and application for known vulnerabilities.
- Penetration testing: These simulate an attack on a provider's network to identify weaknesses in security controls. Internal security teams or third-party consultants can perform pen tests.
- Security audits: These involve a thorough review of security policies and practices to ensure compliance with industry standards and regulations, including access reviews for sensitive data.
- Security information and event management (SIEM): These systems detect and alert on security threats in real-time by analyzing logs from various sources to provide a comprehensive view of the provider's security posture.
- Red team exercises: These exercises simulate an attack by an outside adversary to test a provider's detection and response capabilities. Red team exercises are usually performed by specialized teams that attempt to penetrate a provider's defenses in a controlled and safe manner.

With Revelate's fully customizable platform, you can easily implement the security tests that make sense for your organization.

H3: Encrypting data before uploading it to secure cloud storage spaces

Secure cloud storage providers use a number of encryption techniques to protect cloud-based data before uploading it to their servers. Some encryption methods include transfer layer security (TLS), advanced encryption standards (AES), public key infrastructure (PKI), key management, and hashing.

TLS is a protocol that encrypts data in transit between a user's device and the provider's server, enabling data to be secure during transmission. On the other hand, AES is a symmetric

encryption algorithm that uses a single secret key to encrypt and decrypt before data is stored on the provider's servers.

Like AES, PKI is a system that uses public and private keys to encrypt and decrypt before data is stored on a provider's server, while key management techniques like key rotation, key separation, and key vaulting safeguard encryption keys to protect cloud data.

Hashing is a strategy that generates unique digital fingerprints for pieces of data, allowing providers to use hashing to verify data integrity and detect unauthorized changes.

H3: Implementing secure server connections for data sharing

Cloud service providers should implement secure server connections for data sharing to reduce third-party intervention during data transmission. This is typically done using a combination of encryption and authentication measures, including:

- TLS encrypts data using a secure key exchange mechanism when transmitted from client to server.
- Secure Sockets Layer (SSL) establishes a secure connection between the client and server using a certificate authority to verify the server's identity and encrypt transmitted data.
- Mechanisms for access controls, like authentication and authorization, require users to input credentials, preventing unauthorized access.
- Firewalls protect servers and network infrastructure from third-party intervention by blocking unauthorized traffic and only allowing authorized traffic.
- Performing regular security audits ensures a provider's measures are current and effective.

H2: Safer Data Sharing and Storage with Revelate

Rising cyber security incidents and more data than ever being stored in the cloud underscores the importance of properly securing cloud data. And the dangers of not focusing on data security in the cloud are significant and expensive (remember that $4.35 million?).

Revelate is a secure data platform that helps organizations improve data storage operations, generate more revenue, stay competitive, and secure company and customer data.

Explore how Revelate evaluates and ensures security during data transfer, whether buying or selling data or sharing it with internal data consumers. As a data commercialization and data monetization platform, Revelate can easily operate on top of existing data governance and security layers.

Before and After Analysis:

Length: Reduced word count by eliminating filler and irrelevant content, including an entire section about using a competing tool, Immuta?
Length is currently just over 1300 words. Average word count for top performing pages is 1300.

Outline: Simplified outline with optimized headers.

Other: Added unique CTAs pointing to relevant Revelate security pages.