



SECURITY OVERVIEW

Adobe Brand Visibility

September 2026



About Adobe Brand Visibility

Adobe Brand Visibility is a generative AI-first application for Generative Engine Optimization (GEO), designed to help brands enhance their visibility, accuracy, and influence in AI-driven search environments. Going beyond simply tracking mentions, Adobe Brand Visibility provides insights into brand presence in AI-generated answers, offers prescriptive content recommendations, and automates optimization fixes.

Brand Visibility combines what AI systems say about the customer's brand (via LLM responses), how AI agents and users access the customer's site (via CDN logs, analytics platforms, and operational telemetry data), how accessible and optimized the customer's site content is (via SEO and crawler data) and provides recommendations to improve engagement (for both on-site and off-site opportunities). For a complete list of data sources used by Brand Visibility, see the *Data sources* section below.

Brand Visibility components

Adobe Brand Visibility includes the following components:

- **Brand Visibility User Interface** – Enables customers to configure prompt settings, determine data sources for optimization, and monitor a variety of factors through a range of dashboards, including:
 - **Customer Configuration** – Enables customers to set up categories, topics, and prompts that enable Brand Visibility to tailor insights using accurate visibility, traffic, and opportunity analysis. Customers also set up CDN log forwarding, configure [Optimize at Edge](#) settings, and manage CDN routing configurations in this dashboard.
 - **AI Visibility** – Shows customers a real-time, model-by-model view of how a chosen domain appears in AI-generated answers, including visibility, mentions, and citation metrics. Powered by Semrush Enterprise AIO, AI Visibility enables customers to explore which prompts and topics are driving that visibility and benchmark performance against competitors across markets and models.
 - **Brand Presence** – Helps customers understand how their brand is appearing in AI-generated responses. Powered by Semrush, Brand Presence delivers rich competitive intelligence, broad AI platform coverage, and deep analytics.
 - **Prompt Strategy** – Generates suggested prompts that supplement the customer's own, using the brand profile alongside AI visibility, citation attempt, and synthetic persona signals to surface relevant questions the customer may not have thought to ask. Suggestions must be reviewed and accepted by the customer before being added to the prompt library.
 - **Agentic Traffic Insights** – Tracks bot visits to the customer's website, signaling LLM visibility, including metrics on hits and success rates segmented by market and page type.
 - **Referral Traffic Insights** – Provides visibility into how often users click on the links in AI-generated answers, connecting LLM visibility to real engagement, including metrics on bounce rates and referral sources and regions.

- [URL Inspector](#) – Helps customers understand how website pages are performing, revealing how URLs are cited across prompts and categories and showing trending citations to help identify which pages are working well and which can be improved.
- [Optimization Opportunities](#) – Automatically identify visibility gaps, suggest improvements, and provide prescriptive guidance tailored to the customer's brand for optimal impact. Customers can implement any recommended onsite optimization with a single click.
- [Opportunity Workspace](#) – Enables customers to plan, execute, and track AI visibility optimization initiatives and group related opportunities around a common goal. Through the Impact Measurement engine, Adobe Brand Visibility automates the deployment and measurement of supported opportunity types.
- **Brand Visibility Core Agent** – Processes and analyzes data retrieved from the configured data sources for brand visibility metrics (including mentions, citations, and sentiment in LLM responses), optimization opportunities across owned and external properties, AI agent-driven traffic metrics, and referral traffic data and patterns.
- **Brand Visibility Tools** – Support data collection, analysis, and recommendations through the following services:
 - **Data Retrieval Service** – Monitors and collects data from the integrated and customer-configured first- and third-party data sources.
 - **Semrush AI-Answer Retrieval Service** – Monitors and collects responses from LLM-based assistants for configured prompts.
 - **Semrush AI-Answer Analysis Service** – Processes and analyzes responses collected by the Semrush AI-Answer Retrieval Service using third-party LLM providers¹ to make recommendations.
 - **Opportunity Detection Service** – Identifies actionable insights to improve site and external presence to increase brand visibility in AI search.
- [Optimize at Edge Service](#) – Serves optimized content to LLM user agents at the CDN layer. Customers can preview the changes, deploy them quickly at the CDN edge, and validate that the optimizations are live. Optimize at Edge only processes publicly accessible web content that does not require any authentication or authorization. For supported optimization opportunities, see [Experience League](#).

Accessing Brand Visibility

By default, all users in the organization have read and write access to Brand Visibility. Optionally, customers can limit users to read-only access to Brand Visibility.² If this option is enabled, the customer's Adobe Administrator must add the users for whom they want to grant read and write access to the "Brand Visibility" product profile in the Adobe Admin Console. More information is available on [Experience League](#).

Brand Visibility leverages [Adobe Identity Management Services \(IMS\)](#) to manage user access and authentication.

¹ Adobe Brand Visibility leverages multiple third-party LLM providers to analyze collected responses including, but not limited to, Anthropic Claude, Google Gemini, Mistral, Perplexity AI, and Open AI.

² Contact your Adobe representative to enable this option.

Data encryption

- **In Transit** – All data is encrypted in transit over HTTPS using TLS 1.2 or greater.
- **At Rest** – Any data stored by Brand Visibility is encrypted at rest using AES 256-bit encryption.³

Adobe Brand Visibility security architecture and data flow narrative

The following example illustrates how data typically flows in Adobe Brand Visibility:

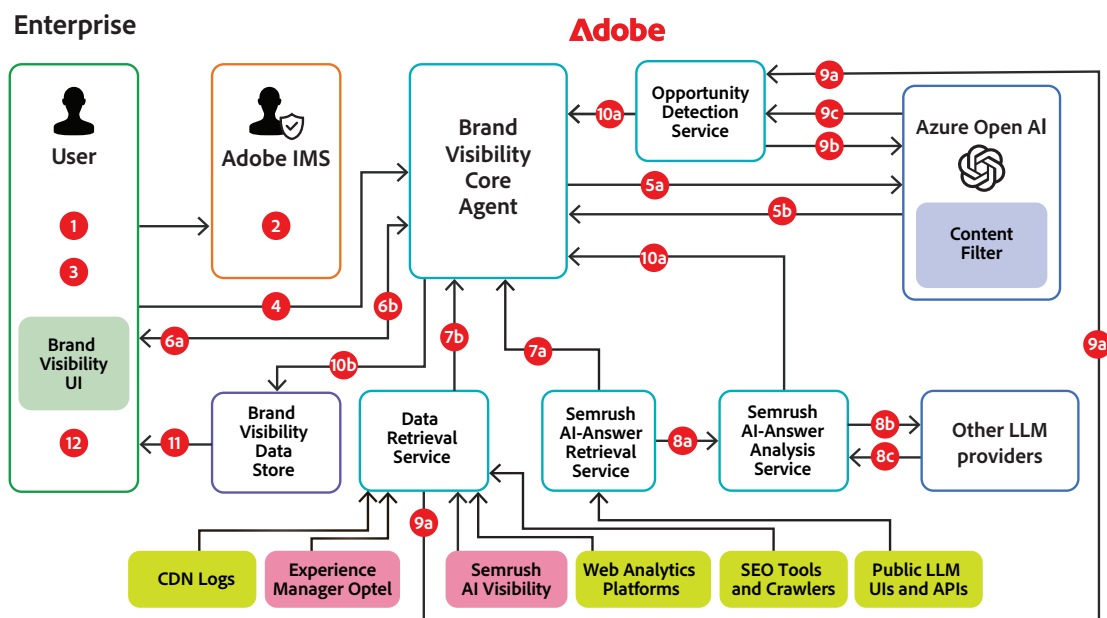


Figure 1: Adobe Brand Visibility data flow diagram

Data flow narrative

Step 1: The user opens Brand Visibility in the AEM Experience Hub or via direct access at <https://abv.adobe.com/> and logs in using their Adobe credentials.

Step 2: Brand Visibility authenticates the user via Adobe IMS (Identity Management Services) and verifies their entitlement to use the service.

Step 3: The user configures their brand in the Brand Visibility user interface, adds prompts (i.e., questions they want Brand Visibility to answer about their website and its visibility in LLMs), selects the LLM-based assistants to query, and connects the CDN used by their website to Brand Visibility for data ingestion.

³ Brand Visibility does not collect or store any personally identifying information (PII).

Step 4: The Brand Visibility user interface sends configuration information to the Brand Visibility Core Agent, which analyzes the information and generates additional suggested prompts.

Step 5a: The Brand Visibility Core Agent sends the additional suggested prompts to Azure OpenAI and **Step 5b:** Azure OpenAI returns category and topic information for the prompts to the Brand Visibility Core Agent.

Step 6a: The Brand Visibility Core Agent sends the category and topic information to the Brand Visibility user interface, where the user can review and accept or reject the suggested additional prompts. **Step 6b:** When the user is satisfied with the configuration, they submit the configuration back to the Brand Visibility Core Agent.

Step 7a: Based on the approved configuration from Step 6, the Semrush AI-Answer Retrieval Service collects data from the selected LLM-based assistants for each configured prompt and forwards the data to the Brand Visibility Core Agent. **Step 7b:** Concurrently, the Data Retrieval Service ingests CDN log data and data from other sources listed in the *Data Sources* section below. The service then processes the logs to compute aggregated metrics (for example, agentic traffic, referral traffic, and crawl failures) and forwards the metrics to the Brand Visibility Core Agent.

Step 8a: The Semrush AI-Answer Retrieval Service forwards the data it has collected to the Semrush AI-Answer Analysis Service, which **Step 8b:** sends the data to an LLM service to determine if the brand was mentioned. **Step 8c:** The LLM service returns the responses to the Semrush AI-Answer Analysis Service.

Note: Brand Visibility does not process or store Personally Identifiable Information (PII) included in text prompts.

Step 9a: In parallel, the Data Retrieval Service forwards collected historical prompt data to the Opportunity Detection Service. **Step 9b:** The Opportunity Detection Service sends historical prompt data where brand visibility is low or has recently declined to Azure OpenAI, which proposes content changes to the relevant pages that help improve or restore visibility. The Opportunity Detection Service also sends information about technical errors resulting from LLM-based assistants' inability to access the customer's site to Azure OpenAI, which analyzes the errors and recommends fixes to resolve the errors. **Step 9c:** Azure OpenAI sends its results back to the Opportunity Detection Service.

Step 10a: The Semrush AI-Answer Analysis and Opportunity Detection Services send the results generated by the LLM service and Azure OpenAI, respectively, to the Brand Visibility Core Agent, which **Step 10b:** stores the data in the Brand Visibility data store.

Step 11: The Brand Visibility user interface retrieves the stored data from the Brand Visibility data store and organizes it into the appropriate dashboards.

Step 12: The user reviews the alerts and recommendations in the Optimization Opportunities dashboard and accepts or rejects each recommendation.

Optimize at Edge security architecture and data flow narrative

The following example illustrates how data typically flows in the Optimize at Edge feature:

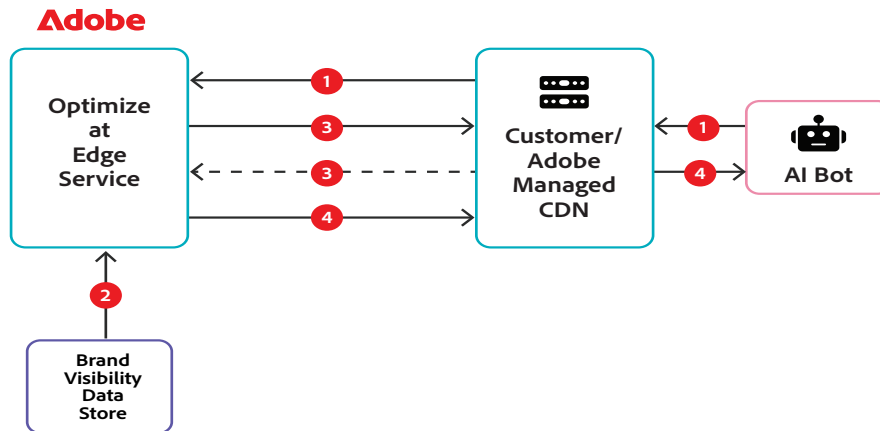


Figure 2: Optimize at Edge data flow diagram

Data flow narrative

Note: Before customers can configure and use the Optimize at Edge feature, they must complete the onboarding process to Brand Visibility. The customer must also configure CDN routing rules to identify agentic traffic based on LLM user-agent strings. Human visitors are not affected by these routing rules.

Step 1: When an LLM user agent (for example, ChatGPT-User) requests a page from the customer's website, the request is routed to the customer's (or Adobe-managed) CDN, which matches the user agent against the configured routing rules and forwards the request to the Optimize at Edge Service.

Step 2: The Optimize at Edge Service retrieves applicable optimization configuration from the Brand Visibility data store in read-only mode. It does not perform write operations to the store.

Step 3: The Optimize at Edge Service fetches the required public page content through the CDN path.

Step 4: The Optimize at Edge Service applies approved optimizations (only for eligible URLs) and returns the optimized response to the CDN, which then serves it to the LLM user agent.

Adobe Brand Visibility and Azure OpenAI

Adobe Brand Visibility currently leverages Azure OpenAI to organize suggested prompts by category and topic, detect opportunities for optimization, and generate suggestions for website improvements. For these activities, Brand Visibility may pass the following data to Azure OpenAI:

- Content from customer's public website
- Configuration data, including brand name and prompts, as well as answers from the LLM-based assistants received by the Data Retrieval Service
- Website performance metrics
- Data from third-party services related to website performance and ranking
- Fragments of website markup and scripts

Adobe never transmits raw CDN logs or any log-level data to Azure OpenAI. Only public website content and de-personalized page-level data is used by Azure OpenAI for prompt/topic categorization.

Adobe has modified the Azure OpenAI abuse monitoring feature so that Microsoft cannot store or conduct human review of the input and output data processed by Azure OpenAI. More information is available at [Azure OpenAI data privacy and security](#).

Content filtering

Adobe leverages the Microsoft Azure AI Content Safety service to moderate hate, sexual, violent, and self-harm content. The service uses Microsoft's collection of proprietary models for content filtering that has both contextual and semantic understanding of text. Adobe has configured the content filter to filter "medium" and "high" severity outputs from the model but not to filter any input.

Other LLM services

The Semrush AI-Analysis Service leverages a variety of LLM services to process the data it collects. For each specific use case, Semrush AI-Analysis Service selects the LLM that it determines is best suited to deliver the required level of answer quality and performance.

All data processed by the Semrush AI-Analysis Service is public data; neither the Semrush AI-Analysis Service nor the LLM services it leverages collect or process customer or PII data.

Model training

Adobe does not use any customer data to train or fine-tune LLMs.

Testing

Adobe teams conduct testing to reduce the potential for biased and harmful outcomes in our generative AI products. For more information on the development and testing processes for our generative AI solutions, please see the [Generative AI Built for Business solution brief](#).

Data sources

Brand Visibility uses several types of data sources as core inputs, depending on the specific customer configuration:

- **LLM response data (input to Brand Presence and URL Inspector dashboards)** – Calls public LLM APIs and crawls public LLM UIs, runs customer-defined prompts as well as autogenerated prompts from SEO signals, and analyzes the responses. Configured by the customer via categories, topics, and prompts in the Brand Visibility UI.
- **Customer CDN logs (input to Agentic Traffic and Referral Traffic dashboards)** – Aggregates HTTP request logs from the customer's CDN⁴ (e.g., Akamai, Fastly, and CloudFront). The logs enable Brand Visibility to detect how often AI crawlers and browsers fetch the customer's pages and measure the traffic health (e.g., success rates, failed URLs, and failure location). Log forwarding is configured by the customer during onboarding. Brand Visibility does not process or store PII at any stage of CDN log ingestion or subsequent data handling. See *CDN log details* below for the subset of fields collected by Brand Visibility.
- **Semrush AI Visibility** – Aggregates data about how a selected domain appears in AI-generated answers across LLM-based assistants, providing model-by-model visibility, mention, and citation metrics, along with prompt- and topic-level detail, enabling customers to benchmark their results against competitors across both markets and models.
- **SEO and crawler insights (input to Optimization Opportunities dashboard)** – Uses a combination of SEO tools and proprietary crawlers in Brand Visibility to understand how the customer's web content is structured and exposed to AI systems. Generates smart prompts and topics for brand presence analysis, detects "hidden" content that AI crawlers might not see, and sends technical gaps (including blocked AI bots, broken pages, and missing structured data). Configured by the customer by defining domains in scope.
- **Web analytics platforms, including Adobe Analytics, Adobe Customer Journey Analytics, and Google Analytics (input to Referral Traffic dashboard)** – Ingests aggregated metrics per URL and referrer post-consent (non-anonymized), such as page views, entries, and bounces; orders, revenue, and conversion indicators; and device and geography breakdowns. This information shows how AI-driven visits perform compared to other sources, quantifies the business impact of LLM visibility, determines conversions and revenue attributed to LLM referrals as well as funnel performance from AI-driven landing pages. Configured by the customer via secured exports and APIs.

⁴ If the customer stores their CDN logs in an observability system, such as Datadog, Splunk, or Grafana, they must manually forward the logs to Brand Visibility. Brand Visibility cannot ingest logs directly from those platforms.

- **AEM operational telemetry⁵ (input to Referral Traffic dashboard)** – Ingests limited samples of metrics per URL, such as visits, bounce rate, consent rate, device, region, channel, and explicit LLM channel classifications. By design, AEM opotel preserves the privacy of end-users by sampling and anonymizing data, giving an approximation of overall traffic. This information helps Brand Visibility estimate how referral traffic is engaging with the brand after landing on the website by checking if the visitor bounced and if a cookie consent banner was displayed. This feature is automatically configured if the customer is using Adobe Experience Manager as a Cloud Service. For more information, see [Experience League](#).
- **Customer's public web content** – When Optimize at Edge is enabled, the service retrieves the customer's publicly accessible web pages directly from the customer's origin to apply optimizations. The service accesses only public content that does not require authentication.

CDN log details

Brand Visibility only ingests a restricted, non-PII subset of fields from CDN logs. Although raw log field names vary by CDN provider, they are normalized and presented in standard format. For more information, see [Experience League](#). Normalized fields are exposed through the agentic view. On the Referral Traffic dashboard, CDN logs are utilized to display page hit metrics.

CDN log analysis is done using Adobe's own ingestion and analytics services and only aggregated metrics are retained. Logs are deleted after processing.

Data refresh

Brand Presence

By default, Brand Presence data is refreshed on a weekly basis. During onboarding, the customer may request daily data refresh instead.⁶

Data is also refreshed when the customer makes the following configuration changes:

- Addition of new prompts – Refresh will occur in the next weekly (or daily) cycle
- Deletion of category or topic – Related data will be removed within 24 hours
- Addition/deletion of brand alias/aliases – Historical data will be reprocessed within 24 hours

Optimize at Edge

Optimized content served by Optimize at Edge is cached with low time-to-live (TTL) settings in the order of minutes.

⁵ If the customer deploys their site using Adobe Experience Manager as a Cloud Service or AEM Sites.

⁶ Additional fees apply.

Data processing and storage locations

Adobe hosts all components of Brand Visibility in AWS US-East-1 (Virginia). The Optimize at Edge Service is deployed globally across CDN edge locations to minimize latency for agentic traffic.

Microsoft hosts the Azure OpenAI Service in Microsoft data centers. Brand Visibility sends all data for processing by Azure OpenAI to the instance in the Azure US-East location. No data is stored in Azure OpenAI.

Adobe does not control the processing locations of public LLM providers leveraged by the Semrush AI-Analyzer Service.

Data retention

Adobe stores the following customer-specific data generated by Brand Visibility in the Brand Visibility data store:

- Brand configuration and execution data, including mentions and citations, is stored until deletion by the customer or upon customer subscription cancellation
- Agentic traffic and referral traffic analysis is stored until customer subscription cancellation
- Identified opportunities and automated improvement suggestions are stored until deletion by the customer or upon customer subscription cancellation
- Optimize at Edge content transformations and deployed optimization configurations are stored until deletion by the customer, rollback of the optimization, or customer subscription cancellation

Questions?

If you have any additional questions about the security posture and capabilities of this or any Adobe product, please contact your Adobe account manager. For all other questions about Adobe's security programs and processes and compliance certifications, see the [Adobe Trust Center](#).