

Data Analytics & Intelligence

In the wake of a data breach – what sensitive data is at risk?

After a data breach, a key step on the road to recovery is to identify and quantify specific sensitive information that has been potentially exposed. State data breach statutes, regulatory requirements, and contractual obligations can all require notification to impacted customers or business partners.

Until now, reviewing this at-risk data to identify sensitive information has been time-intensive, imprecise, and above all — expensive. Legacy techniques designed for eDiscovery could yield false-positive hit rates in excess of 90%. As a result, companies unnecessarily spend thousands of dollars and burn hundreds of review hours to manually sift through data to identify sensitive information.

The Crypsis Illuminator solution offers a streamlined approach to isolating Personally Identifiable Information (PII), Protected Health Information (PHI), and other sensitive data potentially exposed as a result of a breach.

Illuminator combines best-in-class machine learning Artificial Intelligence (AI) with our deep data analytics experience to offer breach victims a better way.

Faster, more reliable, and less expensive

Compared to competing services, Illuminator offers substantial time and cost savings and yields more accurate results.

- Based on thousands of hours of research, development, and experience with the analysis and extraction of data, Illuminator was purpose-built for identifying sensitive information at risk in the wake of a data breach.
- Crypsis combines machine learning AI, natural language processing, and a custom library of search criteria to analyze data in real time. Sensitive data is automatically identified and categorized by data type, consistent with state, federal and international data privacy statutes, effectively eliminating the need for search terms and greatly reducing the amount of required manual review.
- Illuminator is designed to programmatically find sensitive information traditionally identified through manual review, while simultaneously minimizing false-positive results.

CRYPISIS ILLUMINATOR

The industry-leading approach to identifying sensitive information potentially exposed as a result of a data breach.

BY THE NUMBERS

7.5%

Average population of documents recommended for review using Illuminator, out of the total population of documents.

43.5%

Average total reduction of documents recommended for review compared to the eDiscovery search methodology.

\$400,000

Amount saved via Illuminator in one HIPAA matter.

\$20,000

Average savings per matter via Illuminator.

FINDING THE MISSING PIECES

Proactively identifies EU, Australian, Canadian, and other international data.

Captures sensitive data that search terms miss.

A review of 10 GB of email data using traditional methodologies can cost between \$25,000 and \$40,000 depending on the number of hits. **With Illuminator, the cost can be less than \$10,000.**

Customized to your data

No two data sets are the same. Illuminator incorporates a contextual understanding of at-risk data sources, which allows us to eliminate false positives and more precisely drill down on documents relevant for notification purposes.

- We apply a consultative approach to identify expected categories of sensitive information at risk within a data set.
- We work with legal teams to incorporate specific jurisdictional and/or contractual definitions relevant to at-risk data.
- Machine learning AI and natural language processing is augmented with custom-built search criteria specific to each dataset.

Minimize the need for manual document review

The highest cost component in sensitive data identification is the manual document review. Illuminator changes the game by minimizing the number of documents requiring manual review.

- The goal of Illuminator is to provide manual review teams with the smallest, most accurate review population possible.

- Over 95% of the false-positive hits that would otherwise be identified in eDiscovery-based approaches are eliminated upfront and never make it to human review, saving thousands of dollars in review costs.
- Industry standard response rates for sensitive data searches can be as high as 50%. While actual counts vary by data set, Illuminator commonly achieves response rates less than 5%.

Accuracy is everything

Data breach notification often means interfacing with regulators, and/or state or federal authorities, and notifying customers and business partners. Restoring trust depends on getting it right.

- Illuminator incorporates quality control checks at each step in the process and augments best-in-class automation with human review.
- Our data analytics experts review a statistically significant population of the responsive documents, often higher than 10%.
- Illuminator will yield a higher quality notification list, where addresses, phone numbers, credit cards, Social Security numbers and other data points are verified through proprietary checks developed by Crypsis and its partners.

