ENVEIL
ENCRYPTED VEIL

ZeroReveal™ for Mission Operations

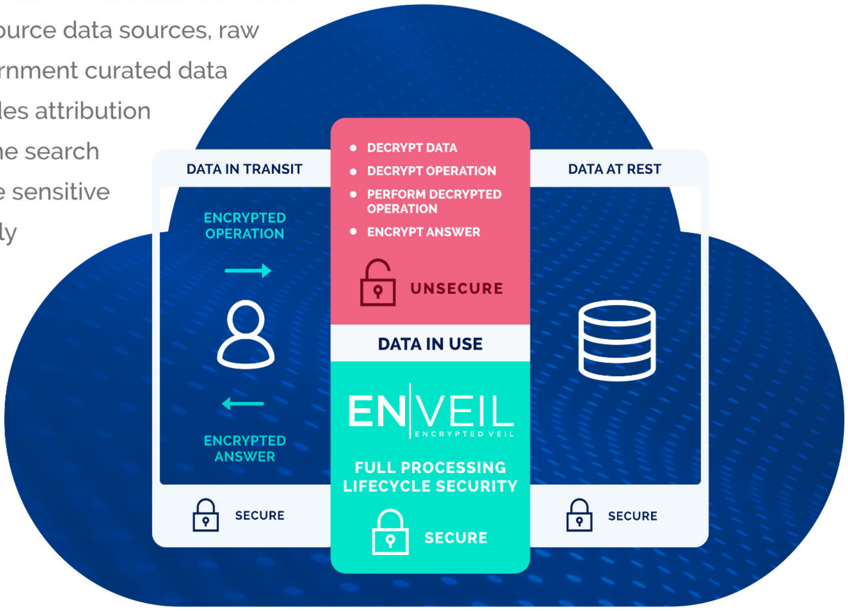
Enabling trusted compute in untrusted locations

Enveil provides the first certified solution for performing searches/analytics/watchlists from classified or trusted domains against sources on untrusted or lower classification domains. **Enveil's ZeroReveal™ solutions** ensure that selectors stay encrypted and nothing is ever revealed during the entire processing lifecycle.

Operations and intelligence analysis methods involving searches of external datasets, including social media datasets, publicly available or open source data sources, raw data inputs collected at the tactical edge, and low side government curated data repositories, are very revealing. This exposure not only includes attribution of the search (who is performing it), but also the content of the search (what you are searching for). This search content may include sensitive indicators and/or classified selectors that would be extremely damaging to national security if exposed.

Currently, there are two main options to avoid this exposure:

- **Searches with sensitive content** are not performed in external datasets, limiting the mission value and usage of the data source.
- **Sensitive operational indicators/classified selectors** must go through the selector release process before being used in external searches which is both time consuming and risk inducing.



Enveil *completely* changes the security paradigm by never decrypting anything, enabling trusted compute in untrusted locations.

UNPRECEDENTED MISSION IMPACT — PUTTING ENVEIL TO USE FOR YOU

Enveil fundamentally changes the paradigm of secure data usage, reduces attack surfaces, and can be used for multiple applications with the potential for high mission impact.

Trusted Compute in Untrusted Locations

Never reveal classified selectors or sensitive indicators when searching third-party or government held data sources.

Secure Use of Publicly Available Information (PAI)

Leverage PAI datasets to derive intelligence using sensitive/classified indicators without ever revealing interests or intentions.

Counterintelligence, Compliance, and Insider Threat

Securely perform CI vetting, compliance checks, or insider threat monitoring without revealing key indicators.

Watchlist Tipping and Alerting

Securely exchange or alert on sensitive information between datasets while data remains encrypted.

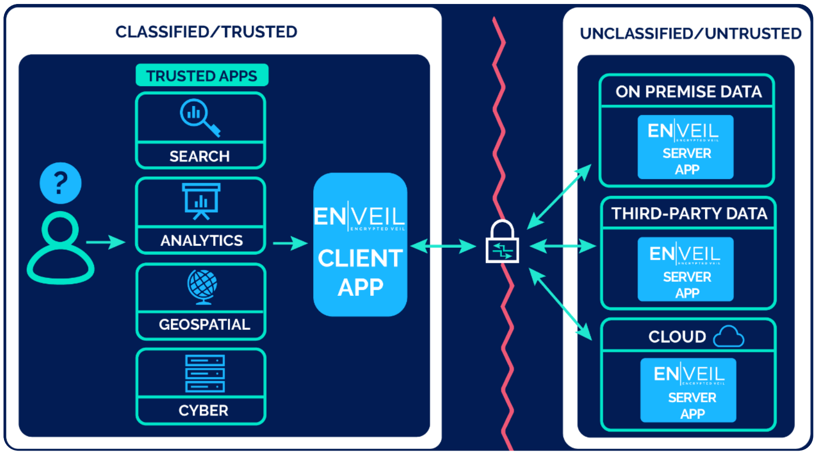
Cross Domain and Interagency Data Usage

Securely utilize datasets in cross domain/interagency environments with selectors of a higher classification, increasing the dataset's intelligence value.

WWW.ENVEIL.COM

A pioneering data security company protecting Data in Use

Enveil provides the first scalable commercial products to protect data when it's most valuable – when it is being used or processed. Whether performing searches or analytics on data you own or seeking information from a third-party data provider, Enveil's **ZeroReveal™ solutions** ensure nothing is ever revealed during the entire processing lifecycle.



CLOSING THE LAST GAP IN DATA SECURITY

Extracting value from data by performing actions such as search and analytics requires decryption, creating critical points of exposure. It's far too easy to assume current security practices already have this covered. They don't. Enveil's ZeroReveal™ compute capabilities close this gap in data security by protecting data while it is being used.

ZeroReveal™ Compute Fabric

Full Lifecycle Security at Scale – First and only scalable commercial solution to enable a ZeroReveal™ security posture, ensuring the content of the interaction, the results, and the data itself are always protected.

Not Intrusive – The capability does not require any changes to a system architecture, data storage format or technology, or application code.

ZeroReveal™ Search

Trusted Compute in Untrusted Locations – Military-grade encrypted search extends the boundary of trusted compute into untrusted locations.

Keep Your Keys – Keys never need to leave the owner's custody even when processing data outside your walls.

Never Decrypt – Data remains encrypted during processing whether within the enterprise, in a third-party data source, or in the public cloud.

Enveil is the **first and only** Data in Use security company to complete the rigorous **NIAP Common Criteria security certification** process, validating the ZeroReveal™ solutions for **nation-state level deployment.** ZeroReveal™ is also a verified component on NSA/CSS's **Commercial Solutions for Classified (CSfC)** list.

ENVEIL COMPLETELY CHANGES THE SECURITY PARADIGM.

Founded by U.S. Intelligence Community alumni, Enveil provides the first and only scalable commercial solutions to **enable full lifecycle security at scale** – allowing organizations to achieve previously impossible levels of data security by ensuring that the content of the interaction, the results, and the data itself are always protected. Enveil's products are **proven in both government and commercial applications** and the company is backed by investors and strategic partners such as In-Q-Tel, Thomson Reuters, Bloomberg Beta, and USAA.

Powered by homomorphic encryption, Enveil's core technology was developed, deployed, and operationalized inside of the National Security Agency to **extend the boundaries of trusted compute** (typically high-side environments or secure enclaves) into untrusted spaces such as cloud environments, open source data repositories, and third-party data services. It has been **implemented at scale in sensitive environments** where analysts work under the assumption the system has been compromised.

ABOUT ENVEIL Founded by a seasoned team of PhD mathematicians and computer scientists from the U.S. Intelligence Community, Enveil is revolutionizing data security by eliminating the Data in Use vulnerability that people have been chasing for more than 20 years. Enveil provides the first and only scalable commercial solutions to enable full lifecycle security at scale. This allows organizations to achieve previously impossible levels of data security – ensuring that the content of the interaction, the results, and the data itself are always protected.