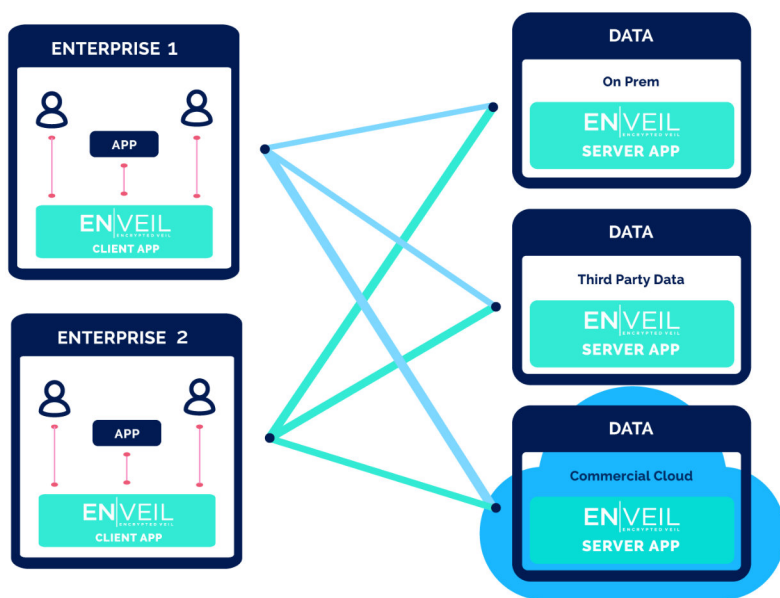


Enveil provides the first scalable commercial products to protect data when it's most valuable – when it is being used or processed. Whether performing searches or analytics on data you own, seeking information from a third-party data provider, or driving revenue by securely monetizing your data assets,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



### 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.

**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.

### 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.



Enveil is the only Data in Use security company to achieve **NIAP Common Criteria security certification**, used by organizations in 28 member countries to assess and certify security solutions. This milestone verifies Enveil's capacity to provide **nation-state level protection in the global marketplace**.

### PUTTING ENVEIL TO USE FOR YOU

Enveil fundamentally changes the paradigm of secure data usage, reduces attack surfaces, and opens the door to untapped use cases across multiple verticals.

 <p><b>Crown Jewel Data Protection</b></p> <p>Ensure security for sensitive data at all times by never decrypting critical data during processing.</p>	 <p><b>Secure Cloud Processing</b></p> <p>Confidently process sensitive workloads/data in the Cloud with Enveil's Never Decrypt security posture.</p>	 <p><b>GDPR &amp; Compliance</b></p> <p>Reduce liability and enhance data governance by never exposing data during processing.</p>	 <p><b>Insider Threat</b></p> <p>Never reveal intellectual property, or PII when searching third-party data sources.</p>	 <p><b>Third-Party Risk</b></p> <p>Securely share data by allowing users to utilize data services without revealing interests/intentions.</p>	 <p><b>Secure Data Monetization</b></p> <p>Monetize data assets and realize new revenue sources without compromising privacy or security.</p>
--	--	---	---	--	--

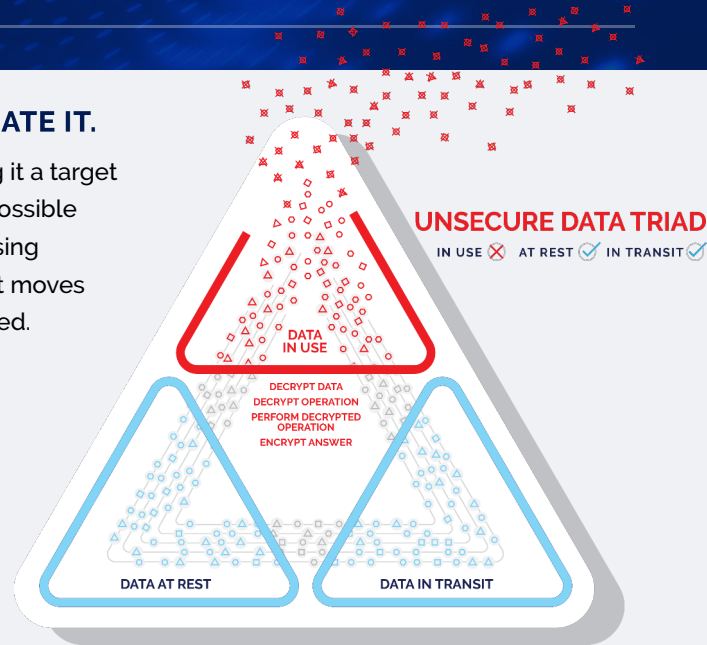
### THERE'S A VOID IN YOUR DATA PROTECTION. WE ELIMINATE IT.

Data is often an organization's largest and most valuable asset, making it a target for all types of adversaries. With attack vectors emerging from every possible angle, organizations must ensure security throughout the data processing lifecycle by securing **data at rest** on the file system, **data in transit** as it moves through the network, and **data in use**, while it is being used or processed.



#### PROCESSING LAYER THREATS WITHOUT ENVEIL:

- ❌ Advanced Persistent Threats
- ❌ Frequency Analysis
- ❌ Compromised Data Environments
- ❌ Insider Threat
- ❌ RAM Scraping
- ❌ Perimeter and Fencing Attacks
- ❌ Side Channel

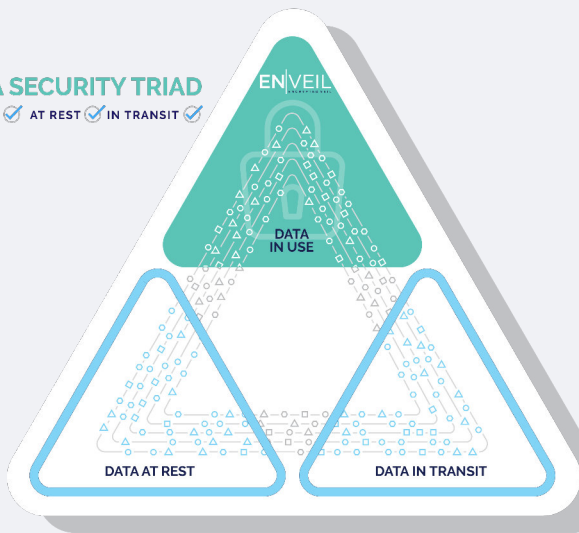


"The range of potential use cases for homomorphic encryption is vast. By focusing on the encryption-in-use space, Enveil complements data-at-rest and data-in-motion encryption to fill a gap in the overall data security landscape."

— Featured Impact Report by 451 Research

#### DATA SECURITY TRIAD

IN USE ✓ AT REST ✓ IN TRANSIT ✓



### GROUNDBREAKING TECHNOLOGY, SEAMLESS INTEGRATION

Enveil allows organizations to analyze, search, and perform calculations on sensitive data without ever decrypting anything, eliminating the risks of theft or incidental exposure. Powered by homomorphic encryption, Enveil **extends the boundaries of trusted compute into completely untrusted spaces**.

Enveil allows organizations to securely use data *where it is* and *as it is* today, **delivering nation-state level security without requiring any system overhauls**. By decoupling from the storage technology layer, Enveil is able to sit above the data, requiring no changes to the underlying environment. Enveil's solution is completely API-based allowing users to interact with Enveil the same way that they interact with their data today.

Best Cloud Computing Security Solution

Winner

2018 SINET 16 Innovator

SINET 16 INNOVATOR

Finalist and Runner-up

RSAC Innovation Sandbox 2017

Revolutionizing data security – and the industry is taking notice.

**NATION-STATE DATA SECURITY IS A PRIVATE SECTOR NECESSITY; ONLY ENVEIL DELIVERS THE 'HOLY GRAIL' OF DATA ENCRYPTION.**

- ✓ **Only NIAP-certified solution** providing nation-state level security in the processing layer.
- ✓ **Protections so effective** that the operations could safely be processed in an environment known to be malicious or actively under attack.
- ✓ **Ultimate safeguard for your sensitive data** while still enabling the value attained through access and use.