WHY NOW?
THE GROWING NEED FOR PRIVACY ENHANCING TECHNOLOGIES

The term Privacy Enhancing Technologies (PETs) has been around for decades and is now experiencing a renaissance as the global awareness, demand, and regulation for privacy increases. At its core, Privacy Enhancing Technologies is a family of technologies that enable, enhance, and preserve the privacy of data throughout its lifecycle. These technologies allow data assets to be securely and privately used, overcoming the very regulatory barriers that have in many ways spurred a renewed interest in their utilization. For organizations, PETs are an innovative path to extracting critical insights without the need to move or replicate data, and enable them to pursue data sharing and collaboration practices while remaining in compliance.

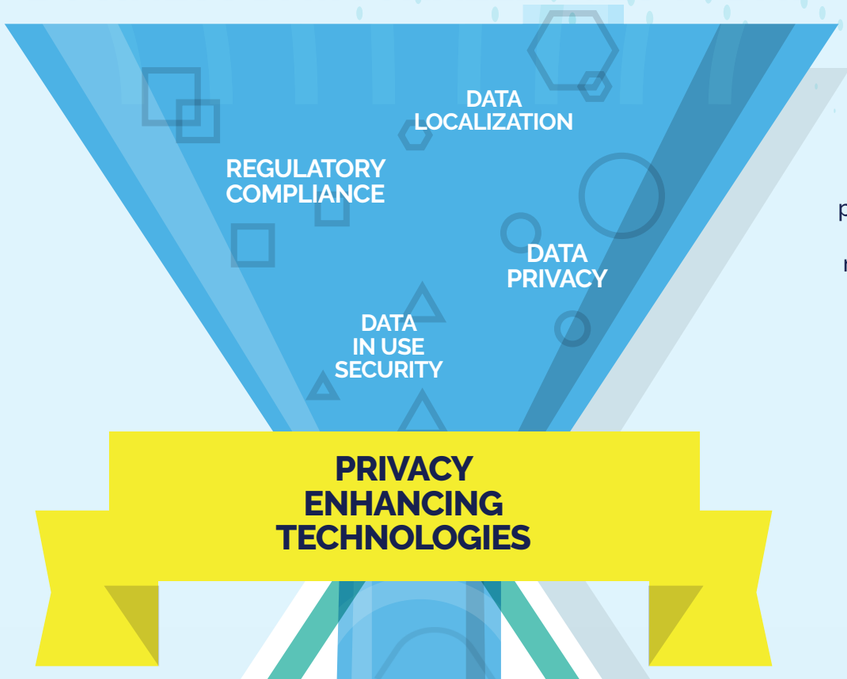
BUSINESS DATA CHALLENGES TODAY

80%

Before year-end 2023, more than 80% of companies worldwide will be facing at least one privacy-focused data protection regulation.*

1m+

By year-end 2022, more than 1 million organizations will have appointed a privacy officer (or data protection officer).*



65%

By 2023, 65% of the world's population will have its personal information covered under modern privacy regulations, up from 10% today.*

$8b

Through 2022, privacy-driven spending on compliance tooling will break through to over $8 billion worldwide.*

*Gartner "Predicts 2020: Embrace Privacy and Overcome Ambiguity to Drive Digital Transformation," | Bart Willemsen, Nader Henein, and Bernard Woo, 14 November 2019

BUSINESS ENABLEMENTS

- SECURE DATA COLLABORATION
- SECURE IOT/ EDGE COMPUTE
- SECURE CLOUD PROCESSING
- SECURE DATA SHARING
- SECURE WATCHLISTS
- PRIVACY-PRESERVING MACHINE LEARNING
- REGULATORY COMPLIANCE
- SECURE DATA MONETIZATION
- INSIDER THREAT

DATA IN USE

SECURE MULTIPARTY COMPUTE

The Secure Multiparty Computation (SMPC or MPC) family of techniques allow multiple parties to jointly operate on data while keeping their individual inputs private. Ultimately, the security and hence privacy of SMPC varies widely and depends on which type is used.

HOMOMORPHIC ENCRYPTION

Homomorphic encryption is the most secure option, providing nation state level security and thus offering the strongest privacy guarantees. Widely considered to be the 'holy grail' of encryption, it allows for computation in the encrypted or ciphertext space.

TRUSTED EXECUTION ENVIRONMENT

The security of Trusted Execution Environments (TEEs) is essentially a perimeter-based security model — in TEEs, the perimeter is very small and exists on the hardware chip itself instead of at a network boundary. It can be risky because, as with any perimeter security model, if you can break through the perimeter, you can gain access to all data within.

YOU ARE HERE.

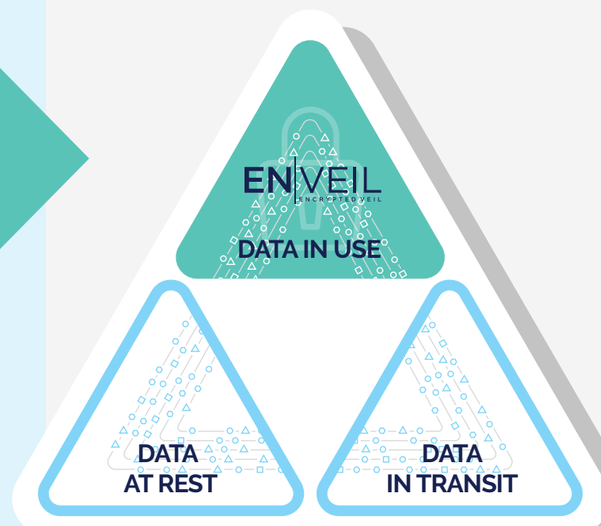
NOT ALL PETs ARE CREATED EQUAL.

While the label itself is intuitively powerful — who isn't in favor of technologies that enhance privacy? — it is also ill-defined and often misunderstood. There are a broad and varied range of business-enabling capabilities powered by Privacy Enhancing Technologies, but not all PETs are created equal.

In order for businesses to fully receive the benefits of leveraging the technologies in this increasingly visible category, they must start by understanding what the label encompasses and which market challenges PETs are most apt to address.

IN CONTEXT:
THE DATA SECURITY TRIAD

PETs KEEP SENSITIVE DATA SECURE DURING PROCESSING BY PROTECTING DATA IN USE



Organizations often need to perform operations such as searches or analytics in order to extract value, which creates points of data exposure. PETs help eliminate this vulnerability by enabling data to be securely and privately processed. This is particularly important when performing operations on PII or other sensitive data in order to minimize regulatory risk.

ENVEIL ENCRYPTED VEIL

Pioneering Data in Use Security

Enveil's business-enabling capabilities for secure data search, sharing, and collaboration protect data while it's being used or processed – the 'holy grail' of data encryption.

Powered by homomorphic encryption, Enveil's ZeroReveal® solutions extend the boundary of Trusted Compute in Untrusted Locations™, allowing businesses to securely derive insights, cross-match, and search third-party data assets without ever revealing the contents of the search itself or compromising the security or ownership of the underlying data. By ensuring that nothing is revealed during the entire processing lifecycle, Enveil completely changes the security paradigm.

Enveil's privacy-preserving capabilities allow organizations to securely use data where it is and as it is today. By decoupling from the storage technology layer, Enveil sits above the data for a straightforward deployment that requires no changes to the underlying environment. Whether performing searches or analytics on data within an organization's walls, seeking information from a third-party data provider, or driving revenue by securely monetizing data assets, Enveil ZeroReveal ensures sensitive search content and its corresponding results are never exposed during the entire processing lifecycle..

TRUST AND GOVERNANCE DECENTRALIZED FRAMEWORK

API-BASED, STRAIGHTFORWARD SOFTWARE DEPLOYMENT

NIAP/CSfC CERTIFIED
NATION-STATE LEVEL PROTECTION

2020 WEF TECH PIONEER
WORLD ECONOMIC FORUM TECHNOLOGY PIONEER

2020 REG TECH 100
REGTECH100 2020
www.RegTech100.com

FINALIST & RUNNER-UP
RSAC INNOVATION SANDBOX 2017

FINANCIAL SERVICES: ENABLING SECURE AND PRIVATE DATA SHARING AND COLLABORATION

2019 Winner Overall (US) & KYC/CDD Use Case (UK)
FCA
Global AML & Financial Crime TechSprint

Each year, large Financial Institutions spend hundreds of millions completing KYC checks on new and existing customers, however, no framework exists to collectively mitigate risk through the sharing of customer risk intelligence across privacy jurisdictions or between entities. This lack of access to existing intel often forces institutions to make risk-rating decisions based on incomplete information. Utilizing its breakthroughs in homomorphic encryption, Enveil worked alongside market participants to develop a flexible and adaptable trust framework capable of facilitating secure and private Know Your Customer (KYC) and Customer Due Diligence (CDD) processes to enhance intelligence-led decision making.

Analysts were able to securely and privately cross-match and search regulated data across privacy jurisdictions in a business-relevant timeframe while ensuring sensitive assets remained protected during processing in accordance with regulatory requirements. The use case validated Enveil's capabilities as a foundational component of a trust framework enabling Financial Institutions to expand data inputs to better understand customer risk and make faster, better informed onboarding decisions. It also laid the groundwork for future intra- and inter-bank applications.

RESULTS & CAPABILITIES

- **Homomorphic Encryption** is ready now and can be implemented in scalable, practical fashion
- **Access** to additional, third-party data sources can be obtained while maintaining strong security and privacy features, customizable business logic, and fully traceable and transparent audit/regulatory control processes
- **Success** of a decentralized data model – participants don't have to move or consolidate data assets
- **Data owners** don't have to change their data environment or re-encrypt their data, shortening the time and cost to value

"Enveil ZeroReveal® solutions enable entities to securely leverage external and cross-jurisdictional data assets in place without revealing the contents/interests of the sensitive search or the results returned.

- ELLISON ANNE WILLIAMS
FOUNDER AND CEO, ENVEIL

Close the last gap in data security.

enveil.com