Paperclip

White Paper

Safe

Protect & Secure Your Data

Paperclip.com

Version 2022.1

Paperclip SAFE Ends the Breach: Protect & Secure Your Data

Cybersecurity and data privacy are under assault—and the hackers are winning to the tune of nearly $5B annually. Perimeter security alone does not protect the most valuable asset of any company… its data.

What's more is that it is becoming harder for organizations to prevent against a data breach as transitions to hybrid and cloud environments take place and technology ecosystems become more complex.

This is where SAFE, a patented privacy enhancing technology developed by Paperclip, offers sea change protection through the use of secure Application Program Interface (API) Encryption, Zero Trust Security, and Shredded Data Security. The SAFE platform delivers steadfast defense against the data breach pandemic no matter if data assets are in use, at rest, or in motion without compromising speed while enabling the fastest and most secure searching.

What is Privacy Enhancing Technology (PET)?

Encompassing a wide collection of technical tools, PET is designed to safeguard the privacy of confidential data through anonymity, opaqueness, inaccessibility, and minimization. As such, SAFE combines patented technologies to solve today's most pressing security and compliance challenges.

SAFE assumes attackers have already breached the perimeter, acquired credentials, and that every API request is actually an attack—SAFE nullifies hacking tools, ensuring database activity remains encrypted, eliminating single key access, and tracking database activity to identify anomalies and respond to potential attacks.

What Sets SAFE Apart

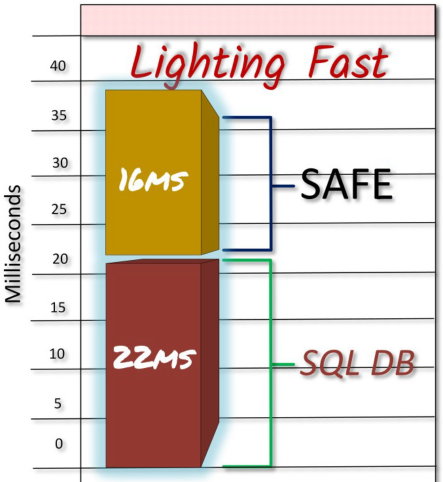
Leveraging Machine Learning Algorithms, SAFE combines crypto technology with advances in data storage and retrieval, resulting in large scale data protection while enabling faster, searchable access.

SAFE empowers organizations to:

- Safeguard confidential data and ensure privacy
- Find and access data at blinding speeds
- Defend against attackers focused on breaking encryption
- Apply multiple key vaults so no one can decrypt data individually
- Mitigate the possibility of experiencing a comprised database, stolen data, operational downtime, reputational damage, and financial loss

Approximately 69% of businesses use API technology to connect with business partners and Software as a Service (SaaS) platforms. Furthermore, approximately 80% of Internet traffic today is machine to machine API messages. Because of the prevalence of API technology and its growing usage, attackers consider API hacking to be "low hanging fruit" and Gartner predicts that this type of attack will become the most-frequent attack vector, causing data breaches for enterprise web applications.

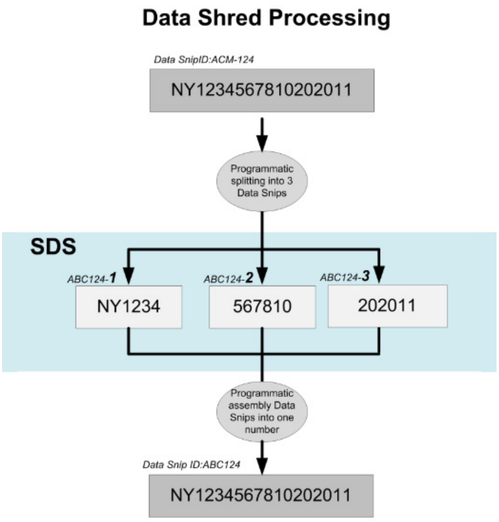
SAFE prevents API hacking because it operates with the assumption that every API request is indeed a threat and should be treated accordingly. SAFE uses Threat Detection and Response (TDR) technology and artificial intelligence to determine the intent of the API request, monitor data behavior, and secure sensitive information, thus preventing API hacking.



Simple SQL Query – SELECT clause & WHERE statement for a 4 million row database with 1,200 SSN search results. MS SQL returned 22ms and after shredding returned in 38ms.

Enable Searchable and Fast Encryption (SAFE)

In order to protect data—in use, at rest, or in motion—it must be encrypted and remain that way. SAFE enables business applications to search, create, read, update, and delete data without having to decrypt it by using patented algorithms. With SAFE, fast and secure searching is delivered while application performance is maintained. Data is protected without an organization losing control.



Shredded Data Storage

Shredded Data Storage (SDS) is built around perfect secrecy for data in use and at rest. SDS operates as the last firewall, ensuring that if data is stolen, the attacker's threat is mitigated as it makes stolen data useless and renders recovery impossible.

Ultimately, shredded data storage is a data destruction technique that involves destroying the keys that allow data to be decrypted. It negates "reverse engineering" methods and techniques used by hackers and makes their classic toolbox obsolete.

Zero Trust Security

Global industry has largely operated on "Implicit Trust" that electronic data and services would not be compromised, that everyone's security was "best practices," and that people would simply behave. However, SAFE operates in a "trust no one" capacity when considering privacy matters. SAFE eliminates a single point of failure through the introduction of multiple key vaults as multiple encryptions are managed. Therefore, no one single party has the ability to decrypt data on their own.

To prove SAFE does what it says, Paperclip partnered with "white hat" hackers, also known as ethical security hackers, to uncover any vulnerabilities within the platform. Conducting white, grey, and black box attacks, we learned:

- SAFE's TDR captured anomalies on hackers using Reconnaissance tactics before they did any harm.
- Shredded Data Storage did not expose any trends or statistics on the database activity.
- Bruteforce attacks were ineffective because data shreds with no context mitigated the attacker's ability to apply rules.

To summarize, the SAFE solution works.

Proven Results

Every company, data owner, and vendor on the planet shares a few elusive goals:

- Realize the power of stored data
- Keep that data secure and protected against threats
- Make the data more searchable, useful, and profitable

SAFE makes these goals attainable.

- SAFE privacy enhancing technology is designed to ensure privacy resilience. Knowing that even with complete penetration and data exfiltration, privacy remains intact and will eliminate the costly effects of a malicious breach.
- SAFE addresses the challenge of data location across borders. SAFE's Trust Security, featuring multiple key vaults, ensures that local laws could not complete data exposure without the data owner's permission.
- SAFE represents the company's safe room for their data when it is attacked. When the SAFE Threat Detection Response triggers, it implies the perimeter and network detection has failed.
- SAFE's database can become the landing technology for on-premises, cloud, and hybrid platforms. SAFE API lends itself to integration with mobile, desktop, and cloud SaaS applications, enhancing confidential data storage and relieving security weaknesses that new technology, such as Internet of Things (IoT), does not address.
- SAFE tells the world you have the future of data privacy and security. Bad actors need not apply.

Paperclip is a global leader in document management and security. Clients that include rapidly growing firms and Fortune 1000 companies trust Paperclip to solve their greatest digital information challenges.

With the introduction of SAFE, Paperclip will continue to revolutionize the ability to protect and manage sensitive business content while preventing against data loss that can lead to a business's ultimate demise.

Now is the time to change the way we look at data security and defeat the breach.

Reach out to Paperclip today with any additional questions you have about SAFE. We are eager to collaborate and provide insight as a trusted partner. Arrange a private consultation now.