# Synthetix Privacy Analyzer

Securing privacy across devices and applications


## What data is exposed from your web/mobile applications?

In today's digital age, privacy has become a significant concern for individuals and organizations alike. With the increasing amount of data being shared and stored online, protecting personal and sensitive information has become more critical than ever. We developed a privacy analyzer technology to analyze and protect users’ privacy.

Synthetix Privacy Analyzer is a set of algorithms designed to analyze and evaluate the privacy practices of websites and mobile applications. It assesses the privacy policies of these platforms and identifies any potential privacy risks and vulnerabilities. Synthetix Privacy Analyzer protects users' privacy at all usage levels, starting at the authentication all the way to website navigation and online

activities. The system protects the user's credentials, identity, location, and additional private information.

One of the primary benefits of our Privacy Analyzer is that it provides users with an objective assessment of privacy practices. Synthetix uses a standardized set of criteria to evaluate the privacy policies of websites and mobile applications, ensuring that the evaluation is consistent and unbiased. This allows users to make informed decisions about the platforms they use and the information they share online. Additionally, Synthetix privacy Analyzer calculates privacy metrics, probabilities of disclosure, and insights about the created fictitious data that is used for user's credentials or personal data.

## Addressing Privacy

Synthetix privacy control includes several key methods to address privacy concerns and protect personal sensitive information.

Strong password analysis: One of the easiest and most effective ways to protect online privacy is to use strong, unique passwords for each account. Synthetix privacy analyzer analyzes each generated, fictitious password to ensure robustness and strength.

Ensuring two-factor authentication: Two-factor authentication (2FA) adds an extra layer of security to your accounts by requiring a code in addition to your password. This helps prevent unauthorized access even if your password is compromised. Synthetix privacy analyzer evaluates each 2FA process to maximize protection.

Machine Learning privacy risks identification: Synthetix Privacy Analyzer mechanism relies on machine learning algorithms to analyze privacy policies and identify potential privacy risks. We use Google's TensorFlow library to create models that analyze privacy policies and provide insights into potential risks. TensorFlow is a popular open-source library that is used across a wide range of

tasks and particularly focuses on the training and inference of deep neural networks for application-specific functionalities. In Synthetix TensorFlow is used to gain insights into the privacy of data in a few ways. The model includes support for differential privacy, which is a technique for adding noise to data to protect individual privacy while still allowing useful statistical analysis. This enables Synthetix to analyze data without compromising individuals' privacy. TensorFlow is also used to detect anomalies in data, which can help identify potential privacy breaches. For example, if a particular individual's data is significantly different from the norm, it may be an indication that an account was compromised. Additionally it can be used to assess the generated fictitious data, determining its strength and reliability.

Encryption: One of the key technological solutions to maintain online privacy protection is encryption. In order to provide a robust privacy protection Synthetix uses encryption techniques to secure authentication, and internal modules communications. It ensures secured authentication, preventing information leaks and unauthorized access, including interception by third parties.

Mathematical algorithms that calculate privacy metrics estimations like probability of disclosures, username and passwords strengths, vulnerabilities predictions and simulations. These algorithms are an integral part of the ongoing security scanning to detect unusual anomalies, alert and mitigate.

Synthetix encryption is implemented using common practice encryption algorithms, such as AES (Advanced Encryption Standard), and RSA (Rivest-Shamir-Adleman). These algorithms use complex mathematical formulas to encrypt and decrypt data, ensuring that only the intended recipient can access the information. While encryption is a powerful technology for protecting online privacy, it is not foolproof. Hackers and cybercriminals can still use various techniques to gain access to sensitive data. That is why we implemented a second layer of security within Synthetix, particularly for authentication and information access, The Honey Encryption technique.

## The Honey Encryption Advantage

Honey encryption is a relatively new encryption technique that can be used to protect user's privacy. Unlike traditional encryption methods that aim to prevent unauthorized access to sensitive data, honey encryption is designed to deceive attackers by providing false but believable data.

Honey encryption works by creating fake data that is similar to the real data. When an attacker tries to decrypt the fake data, they are presented with what appears to be valid information, but is actually meaningless. This makes it difficult for attackers to determine if they have successfully decrypted the data or not.

One of the main advantages of honey encryption is that it can protect users' privacy even if the encryption key is compromised. Traditional encryption methods rely on the secrecy of the encryption key to protect the data. However, if the key is compromised, the data can be easily accessed. With honey encryption, even if the attacker has the encryption key, they will still be presented with fake data, protecting the real data from being accessed.

Synthetix uses Honey encryption to protect user's privacy in various ways. First it is used to protect passwords and authentication. Using this method, brute force attackers will be presented with fake passwords that look real, making it difficult to gain access to user accounts. Secondly, it is used to protect the central database which contains user’s information, fictitious datasets and operational data. Synthetix module’s communication channels are additionally equipped with Honey Encryption in order to increase security, preventing data theft, DoS or tampering. Honey encryption is another security layer to increase Synthetix cybersecurity measures, enabling personal data robust protection, anonymity, and superior privacy.

## Conclusion

Synthetix is equipped with robust methods and techniques to provide privacy protection. Its privacy analyzer processes each of the application's activities to ensure data protection, anonymity, and safe, reliable operation. Honey encryption is one of the powerful methods that is used to protect privacy and security. It works by providing attackers with fake but believable data, protecting the real data from being accessed. It is used to protect passwords, databases, and other sensitive data by deviating attackers with deceived data. In general, Synthetix privacy analyzer is a set of systems and methods to ensure sensitive data protection, while alleviating privacy concerns throughout the data life cycle. The Privacy Analyzer is an ongoing, real-time, monitoring and analysis security tool, that checks privacy risks, and analyzes the information that is exposed throughout online activities, providing alerts, reports, and mitigations. Additionally, it calculates privacy metrics, and disclosures probabilities and generated fictitious data strength.