white paper

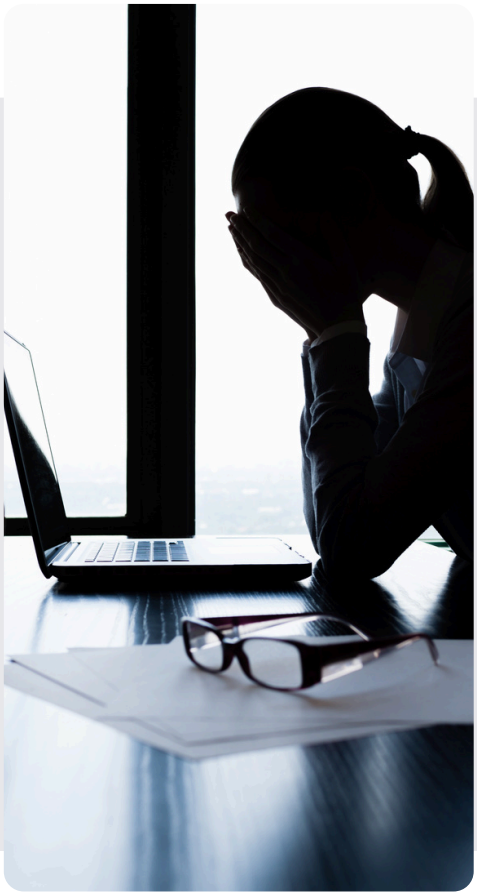
ANONYOME LABS

Inside the Anonyome Platform

An Identity-Focused SaaS Service, Based on the Pioneering Identity Proxy, Scalable to Millions, and Used by Fortune 100 Companies

www.anonyome.com

Personal data is currency, and users have lost control of it.



Personal data is currency on the internet. Web service providers offer so-called free services in exchange for users' valuable personal information, or they sell their users' information as an extra income stream. Digital surveillance on today's internet means users quickly and easily lose control of their currency and it's used for everything from serving them personalized ads to adjusting their insurance premiums and influencing their political preferences.

What's more, personal data is currency for bad actors. Most people worldwide have already had their personal data stolen:

1. In the first half of 2024, the total number of US data breach victims surpassed 1 billion —a 490 per cent increase from the same time last year.
2. In the United Kingdom, 30 million people or 55% of all adults have had their data stolen.
3. Two-thirds of Australians experienced a cyberattack or data breach in the 12 months up to October 2024. Half of those were hit more than once.
4. Across Europe, 2,289,599,662 known records were breached in 556 publicly disclosed incidents in the short time between November 2023 and April 2024.
5. In the Middle East, the UAE's public sector alone averages 50,000 cyberattacks every day, with the number of attacks on the private sector possibly double or triple that number.

Empowering Users to Protect Their Privacy:

The services collecting user data don't always recognize the harm they're doing to users, and users don't always know the data traps they're walking into every time they go online. Since most people have 200+ accounts and visit a myriad of websites daily, the attack surface for exploitation is huge.

It's time to gives users a powerful way to protect their personal information and identity. Enterprises that make it easy for their customers to reclaim control of their data can profit significantly.

Anonyome Labs builds easy-to-use privacy and identity protection tools, available through its identity-focused SDK development platform. Let's go inside the Anonyome Platform.

Identity proxies solve the privacy and identity protection problem:

Anonyome has pioneered an identity proxy and put it at the centre of the Anonyome Platform. Proxies (e.g., VPN, NAT, TOR) are a well-known and well-accepted part of the enterprise security landscape. They're commonly used as an intermediary buffer between the user and the services they access. Proxies establish a user-controlled layer of security and privacy protection that is not possible with direct connections.

Likewise, Anonyome's identity proxy, which we call a persona, serves as the protective buffer for the user, shielding their actual identity and personal data from surreptitious collection, use and abuse. But that's not all: each identity persona acts as a sandbox environment in which activity-specific identity elements and internet activity data can be quarantined. This compartmentalization paradigm prevents the sharing of identity and activity data elements across personas. The user can separate or silo their activities and data and, importantly, disrupt the efforts of data aggregators and data brokers who profit from creating and selling full pictures of users' public and private lives.

As an example, Figure 1 shows how a user might create a separate identity persona for each of their online activities: shopping, travel, donations, selling, work, home, and family and friends. Each of these personas can independently leverage the Anonyome Platform for everyday services, such as email, telephony, virtual cards, VPN, encrypted communications, identity wallet, password manager, and safe browsing.

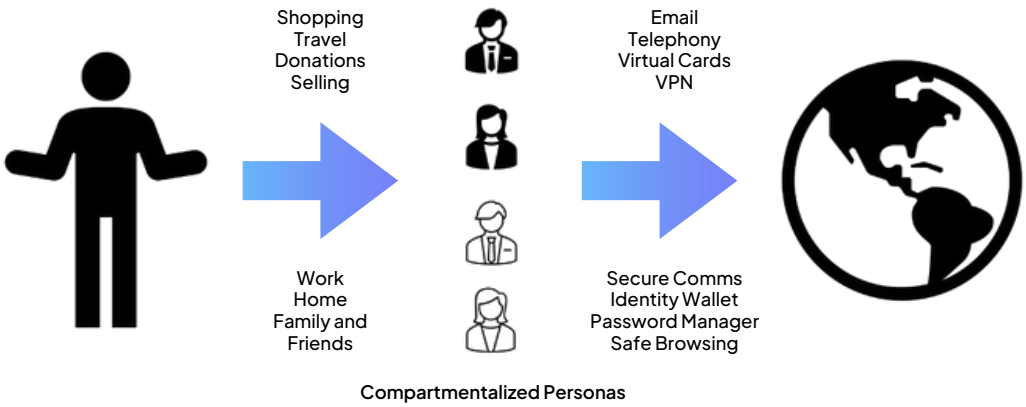


Figure 1: Using personas as identity proxies for all parts of life

Is this type of identity sandboxing also used in the offline world? Absolutely. A simple example is an author using a nom de plume to shield their actual identity: Mark Twain (Samuel Clemens), Robert Galbraith (J.K. Rowling), Richard Bachman (Stephen King), Dr Seuss (Theodore Geisel), and Agatha Christie (Agatha Miller) are famous examples. Motivations for using a nom de plume vary from book marketing to writing in different genres, but a common reason is that it gives the author personal privacy.

Personas put a stop to data correlation

Data brokers and aggregators typically use ubiquitous communication identifiers to correlate user data: email addresses, phone numbers, credit cards, social media handles, and so on. Online interactions are typically captured as browser cookies that are usually linked to one or more of a user's communication identifiers. Data aggregation services can readily link data collections from a range of services through these common communication identifiers.

Identity proxies or personas disrupt and prevent the correlation and aggregation processes by giving the user different communication identifiers and a separate browser cache than they would normally use. While data surveillance activities will still collect data from the personas, they cannot correlate that data since there are no longer any common identity elements shared among personas.

Users can easily and privately communicate using their personas. Figure 2 describes the communication processes and capabilities available to personas from within the Anonyome Platform. It also outlines the structure of the Anonyome Platform.

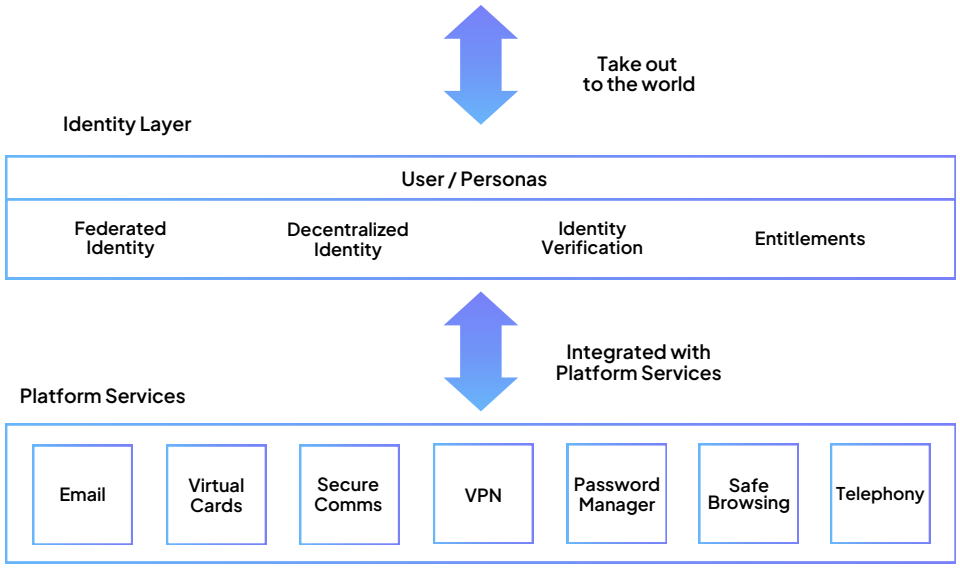


Figure 2: Communication processes and capabilities, and platform services available to each persona, through the Anonyome Platform.

The platform's identity layer has a suite of identity-related services that allow users to tailor their personas to their specific needs. These identity services integrate with external enterprises as well as with internal cybersecurity and privacy services.

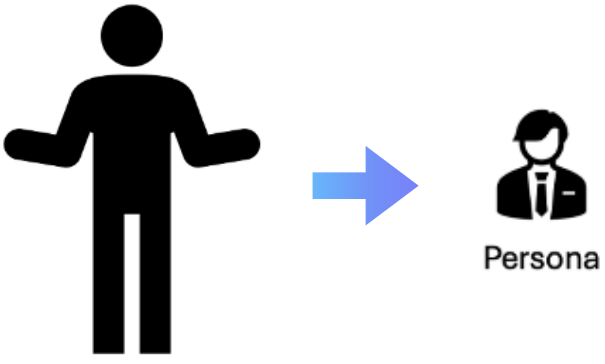
The platform's identity layer provides the personas' cybersecurity and privacy capabilities

The well-integrated **identity layer** provides all the cybersecurity and privacy capabilities that personas use, and includes the following sub-elements:

User/personas :

The platform's identity data model provides users with one or more personas. Many users will typically create one persona that represents their actual "legal identity" with real identity attributes that can be confirmed through identity verification, and then other personas as needed to compartmentalize their activities, such as travel, health care, shopping, selling, donations to charities, and so on. The user can customize each persona to represent and protect those activities.

The full set of persona identity attributes includes an email address, communication handles, phone number, verifiable credential, password manager vault, safe browser instance, virtual payment card number (one time use or refillable), and VPN account. These identifiers (see Figure 3) are contained within the identity layer, and integrated with the platform services layer that manages all the privacy and cybersecurity capabilities of personas.



Persona Capability	Persona Identity Attribute
Email	Email Account
Secure Messaging	@handle
Secure Voice	@handle
Secure Video	@handle
Telephony	Phone Number
Identity Wallet	Verifiable Credential
Password Manager	Vault
Safe Browser	Browser Instance
Virtual Cards	Card Instance
VPN	Account

Figure 3: Persona-based identity attributes and privacy and cybersecurity capabilities within the Anonyome Platform

Federated Identity:

The Anonyome Platform integrates with contemporary enterprise identity providers (IDP) and implements the leading federated identity management protocols OAuth, OpenIDConnect, and SAML. This integration allows users to create native identities within their enterprise's identity system and bridge them with the Anonyome Platform to integrate with the various persona-based services. Similarly, the Anonyome Platform can also serve as the main identity provider to deliver persona-based identity functionality that integrates with external service provider platforms.

Decentralized Identity

An emerging technology field known as decentralized identity (DI) introduces a host of new cryptographic capabilities that allow users to more securely interact with enterprise systems and each other. The core DI components include decentralized identifiers (DIDs), verifiable credentials (VCs), and an identity wallet. The identity wallet serves as a user-managed encrypted datastore that creates and manages cryptographic key pairs and DIDs, and allows the user to receive, store and present verifiable credentials to prove their identity or right to physical or digital access to certain services, such as education, health care, driver licensing, and single sign-on.

Critical cryptographic actions such as key exchange and key rotation are masked from the user so the user benefits from strong security without having to see the potentially overwhelming cryptographic operations. The Anonyome Platform's DI service provides a full suite of verifiable credential issuance and verification capabilities. The platform's identity wallet and issuance/verification services support the leading credential exchange protocols (e.g., DIF DIDComm, HyperLedger Aries, OpenID4VC) and leading credential formats (e.g., AnonCreds, W3C Credentials, SD-JWT).

Identity Verification

Identity verification is the process of confirming the stated identity of a user. It is used in finance and other services to prove age and other protected information. The user provides evidence of their legal identity, such as a driver license, passport or other legal document, and performs a "liveness" test. The platform can combine identity verification with the issuance of a verifiable credential that the user can store in their identity wallet and use whenever they need to prove their identity or right to access a service.

Entitlements

Entitlements stipulate the level of services or quantity of resources that a user (or their persona) is authorized to use. Entitlements are verified when the user is accessing the Anonyome Platform's cybersecurity and privacy capabilities. As an example, email service entitlements may specify the number of email accounts the user can create and the maximum size of their email storage. When used with the federated identity management processes, entitlements can be federated from the enterprise's identity provider and embodied within Anonyome's platform services.

Each persona has secure email, payments, telephony, password manager, VPN and more .

The scalable cybersecurity and privacy services within platform services allows the user to interact privately and securely. Each service is published as a set of SDKs (iOS, Android, and web) which includes service-specific sample apps and documentation.

Each persona has:

Email: A full-service email inbox from which the user can send and receive email with any email-compatible service without divulging their actual personal email accounts

Virtual cards: A refillable or disposable virtual credit card which the user can use in lieu of their actual credit card

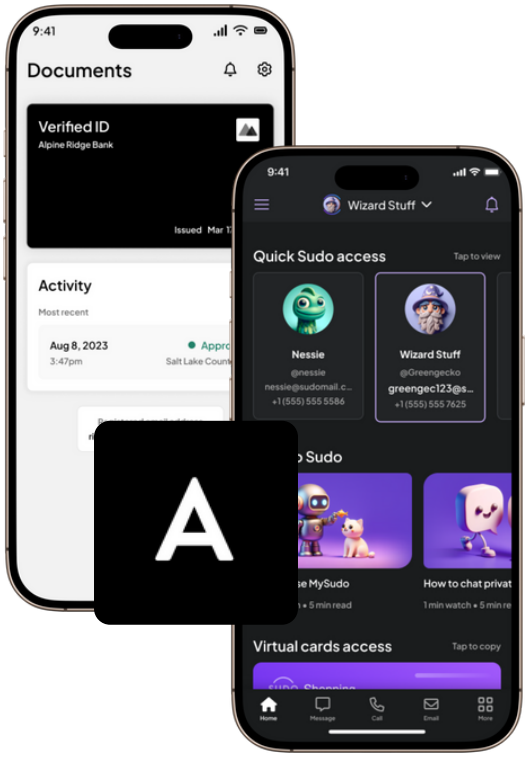
Secure communications: End-to-end encrypted (E2EE) messaging, voice communication, and video services. The messaging service supports 1:1 messaging, group messaging, as well as private and public communication channels. The user can also choose a different handle for each of their personas, which they can use in lieu of their actual name.

VPN: A VPN service to protect the user's device IP address (e.g., desktop, laptop, mobile phone) and encrypt their communications between their devices and the VPN service. This prevents the ISP or another 'man-in-the-middle' eavesdropping.

Password manager: A password manager to securely store, autofill, and organize their logins (usernames and passwords), other credentials, and second factor authentication data for accessing their many online accounts

Safe browsing: A compartmentalized private browser with both site reputation and ad/tracker blocking capabilities. The security cache for each browser is persona-specific and separate from the security caches that their other personas' browsers use. As the user switches between personas, the persona-specific security cache is swapped in and out so that a persona can benefit from data within its own security cache (e.g., staying logged into websites) without cross-contaminating persona-specific data from other personas.

Telephony: A fully functional mobile number that supports ingoing and out-coming calling, ingoing and out-coming SMS/MMS, and even voice mail, so the user can make calls and send messages without divulging their personal mobile number.



The Anonyome Platform is a SaaS service, scalable to millions and used by Fortune 100 companies.

The Anonyome Platform is delivered using a software as a service (SaaS) paradigm. Anonyome's SaaS systems deliver individual cloud environments that are configured for each customer and feature a 24x7 customer support service that adheres to very strict SLA requirements.

What's more, Anonyome built its platform using the latest in serverless computing and cloud native technologies, to scale to millions of users. Several large Fortune 100 companies are already using the platform environments, proving scalability and how well the platform can manage large user numbers.

Interested in integrating the Anonyome Platform's privacy and identity protection solutions into your organization?

Schedule a demo today!