

Own the Future of Digital Privacy

PureVPN White-Label Digital Privacy Protection Platform

- Continuous Exposure Monitoring
- Automated Privacy Remediation
- Privacy Operations at Scale

www.purevpn.com/white-label

Our Infrastructure Foundation

Founded in 2007, PureVPN has built and operated large-scale privacy and security platforms serving millions of users globally. Over 18+ years, we have evolved beyond consumer products into a Partner & Enterprise ecosystem that enables global brands to embed privacy, identity protection, connectivity, and security services directly into their products.

Powering Global White-Label & OEM Digital Services

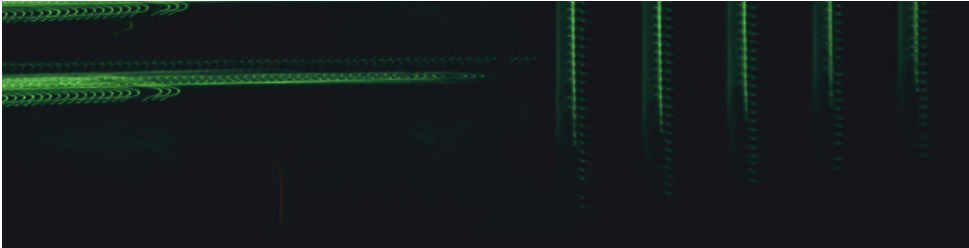
Today, through our Partner & Enterprise ecosystem, we empower global brands to launch and scale consumer-facing digital services powered by **privacy, identity protection, exposure intelligence, connectivity, and security services.**

2007
Year Founded

300+
Global Team

20+ Million
Users Protected

150+
Countries Served



Millions

of exposed consumer identity
records circulating online



Always-On

identity exposure persists until
actively monitored and suppressed



Continuous

re-indexing and resurfacing
of consumer identity data

MARKET REALITY

Privacy Has Become An Always-On Digital Service

Personal information continuously spreads across **data brokers, public identity ecosystems, credential breaches, infostealer malware logs, people-search platforms, and dark web marketplaces**, often without consumer visibility or control.

Identity exposure is no longer limited to isolated breach events. Information now moves continuously across surface web ecosystems and underground intelligence sources, creating persistent privacy and security risks.

This is driving growing demand for identity exposure monitoring, dark web intelligence, privacy remediation, and embedded privacy protection experiences across telecoms, fintechs, cybersecurity products, and consumer digital ecosystems.

Why Digital Privacy Is Changing

1

Shift Toward Identity Protection Services

Consumers are becoming increasingly aware of how exposed their personal information, credentials, and identity data are across digital ecosystems.

2

Always-On Identity Exposure

Identity information continuously spreads across data brokers, breach datasets, infostealer ecosystems, people-search platforms, and dark web intelligence sources.

3

Privacy Expectations Are Evolving

Users increasingly expect privacy, identity monitoring, and exposure protection capabilities embedded directly into the products they already use.

4

Privacy Is Becoming Infrastructure

Telecoms, fintechs, cybersecurity platforms, and digital brands can integrate privacy remediation, dark web monitoring, and identity protection directly into their ecosystems, creating new engagement and monetization opportunities.

The Next Evolution of Digital Privacy

Building The Foundation For Modern Privacy Experiences

As digital identity exposure expands across public and underground ecosystems, privacy services must evolve beyond isolated features into connected, continuously operating experiences.



Exposure Visibility

Consumers need visibility across data brokers, breach datasets, dark web intelligence sources, and public identity ecosystems.



Continuous Protection

Privacy and identity exposure evolve continuously and require always-on monitoring and lifecycle management.



Connected Workflows

Discovery, monitoring, remediation, and protection work best when operating as a unified privacy experience as one solution.



Embedded Experiences

Modern brands require privacy capabilities delivered through APIs, SDKs, white-label platforms, and native application experiences.

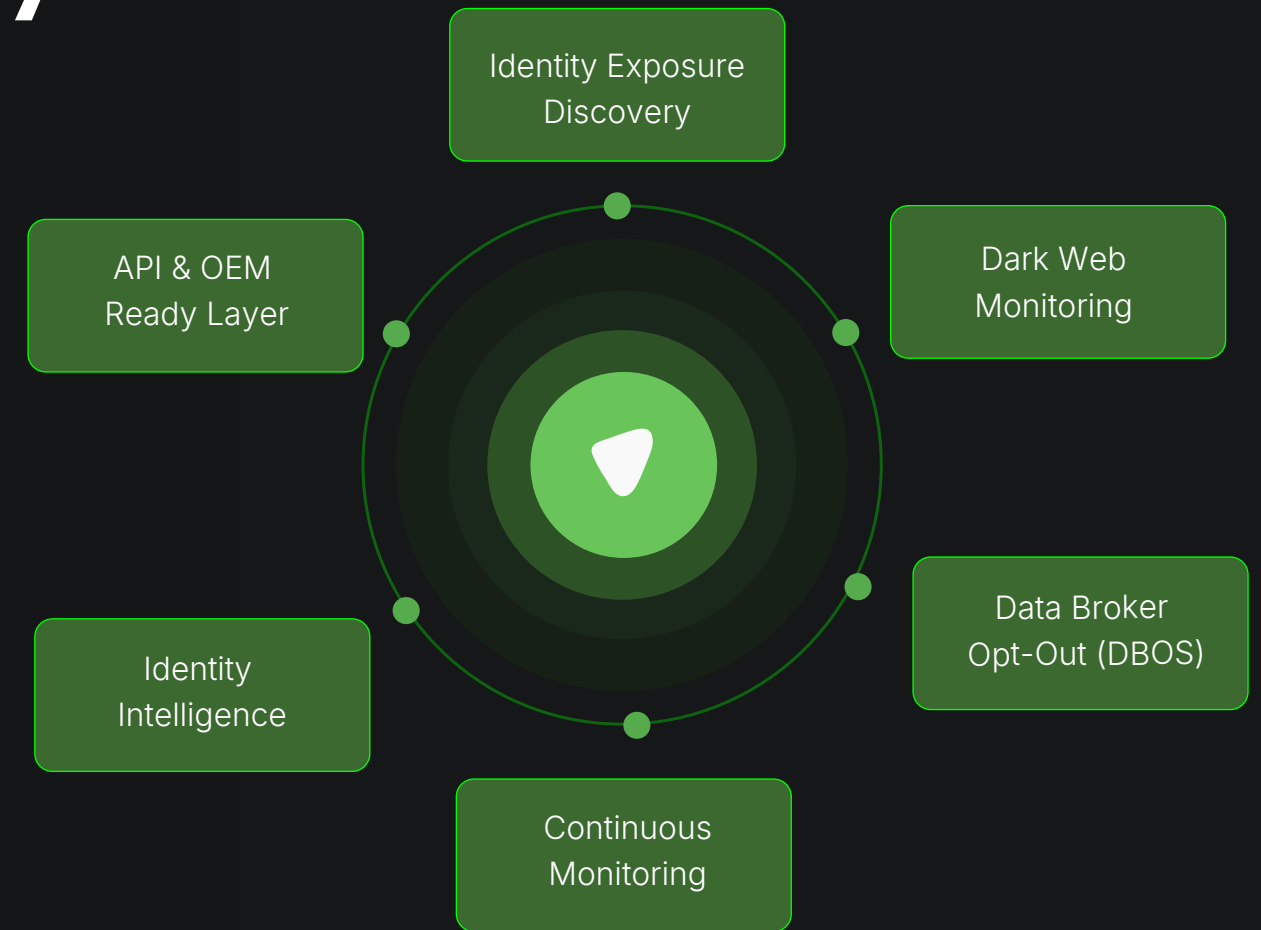
One Platform. Multiple Identity & Privacy Capabilities

Introducing Digital Privacy Protection Platform

Digital Privacy Protection combines **identity exposure intelligence**, **dark web monitoring**, **privacy remediation**, and **continuous lifecycle management** into a unified OEM-ready platform.

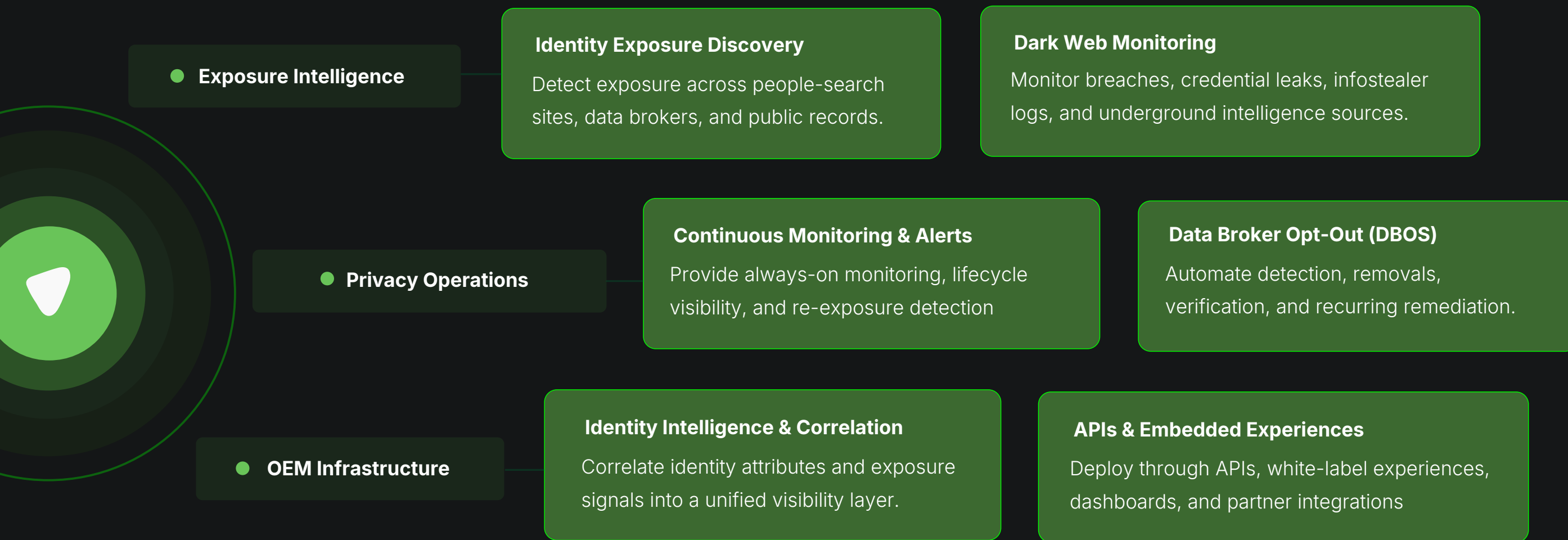
- ✓ Unified Identity Exposure Visibility
- ✓ Continuous Monitoring & Protection
- ✓ Embedded OEM Experiences

Build once. Deploy across telecoms, fintechs, cybersecurity platforms, and consumer ecosystems.



How We Power Digital Privacy Protection

Powered by our identity orchestration layer that connects exposure intelligence, remediation, and OEM deployment into one platform.



How it Works

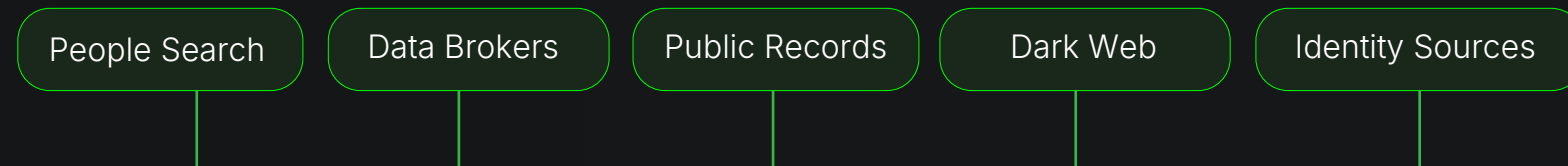
Identity Exposure Intelligence

Unified Identity Visibility Across Digital Ecosystems

Digital Privacy Protection continuously discovers identity exposure signals across public and connected ecosystems to help users understand where their information exists and where risk originates.

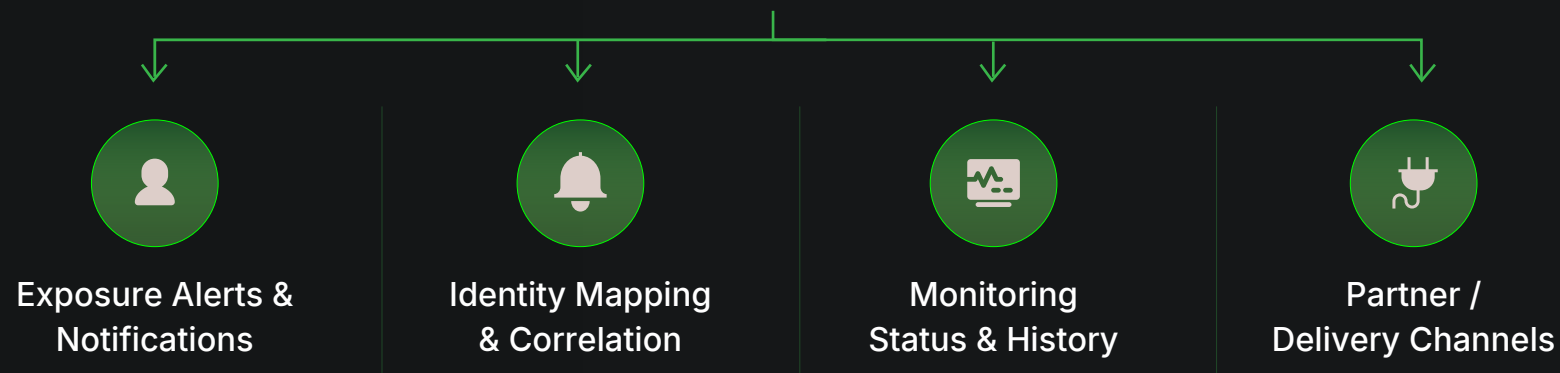
- ✓ **Exposure visibility across public ecosystems**
- ✓ **Correlated identity intelligence**
- ✓ **Risk indicators and exposure validation**
- ✓ **OEM-ready deployment under partner brands**

Exposure Intelligence Sources



IEX Discovery Engine

Correlation · Deduplication · Identity Matching



Partner Experience (White-Labeled)



Partner Apps



Partner Dashboards



Partner Notifications

How it Works

Real-Time Dark Web Monitoring

Digital Privacy Protection continuously monitors underground intelligence sources to identify credential exposure, breach activity, infostealer risks, and emerging identity threats.



Enterprise-grade exposure intelligence delivered through fully branded partner experiences.

How it Works

Data Broker Opt-Out Service (DBOS)

Automated Privacy Remediation Across Broker Ecosystems

DBOS automates the complete privacy remediation lifecycle. Exposure is discovered across broker ecosystems, removal requests are orchestrated and tracked, suppression outcomes are verified, and evidence records are generated to provide visibility, accountability, and continuous protection.

- ✓ **Discover exposed identity listings**
- ✓ **Orchestrate and track removals**
- ✓ **Verify suppression outcomes**
- ✓ **Generate evidence & audit records**
- ✓ **Continuously re-monitor exposure**



How it Works

The Privacy Protection Lifecycle

Discover exposure, monitor risk, automate remediation, verify outcomes, and maintain continuous protection through one unified platform.

Lifecycle Flow

1 Discover Exposure

2 Monitor Exposure

3 Assess & Prioritize Risk

4 Orchestrate Remediation

5 Verify & Generate Evidence

6 Continuous Protection

Identity Theft Protection

Stay one step ahead of identity theft by detecting your data on the dark web and removing it from brokers.

Dark Web Monitoring



07

New breaches found

Monitored assets: 1/5



Email Address

jane1@gmail.com

02 Breaches



Credit Card

**** * 421

0 Breaches

Data Removal

Platform Outcomes



Exposure Intelligence



Real-Time Alerts



Remediation Tracking



Verified Evidence



Activity Timeline



Continuous Protection

APIs Enabled For:



Partner Dashboards



Partner Apps



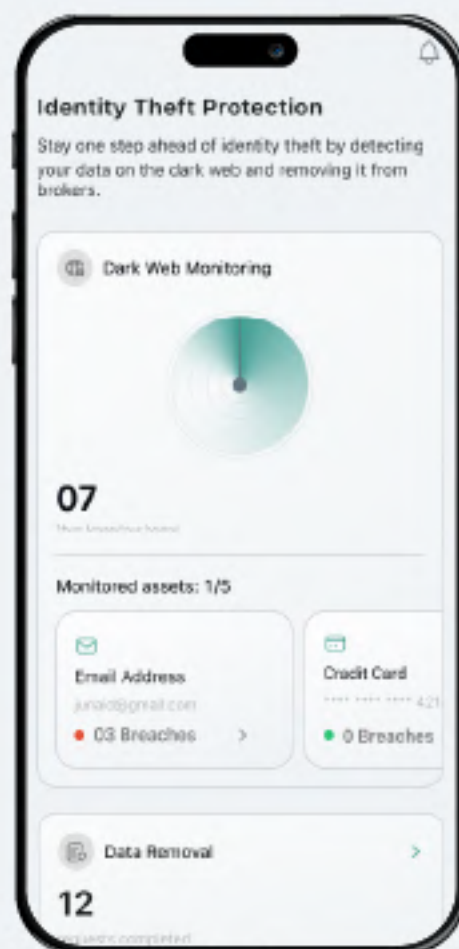
Partner Notifications

Identity Exposure Intelligence

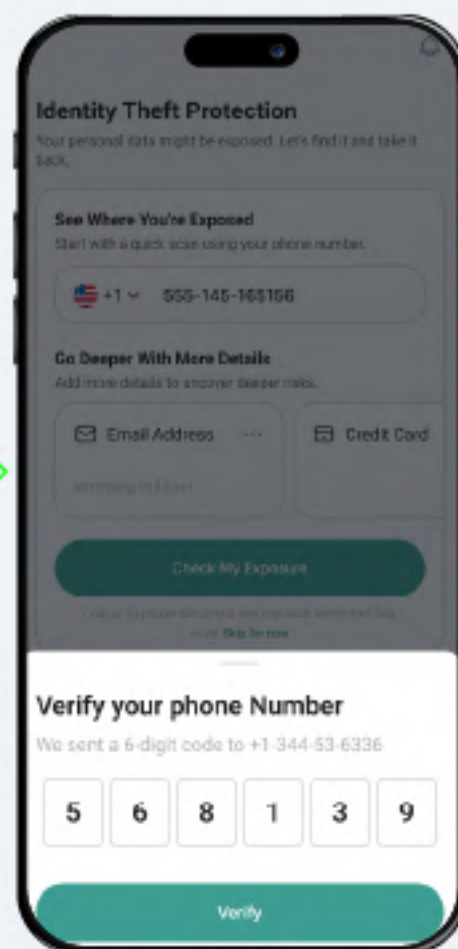
Discover, correlate, and prioritize exposed personal information across public ecosystems.



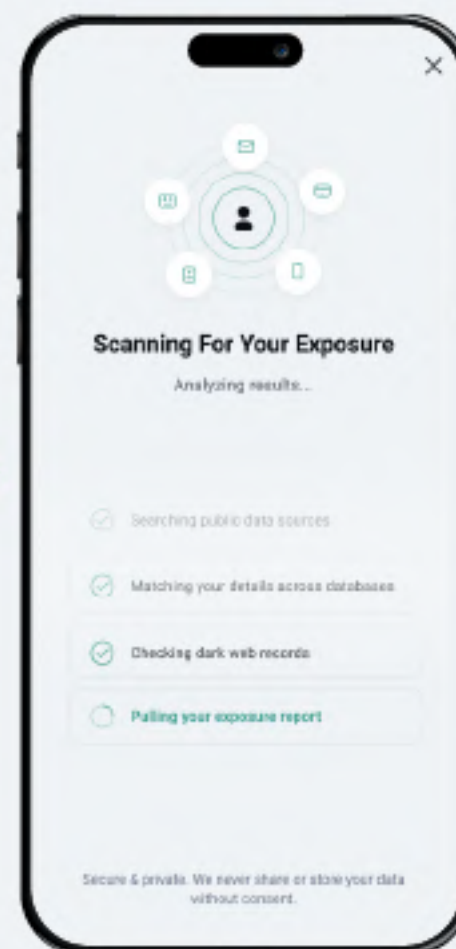
Recommended Flow



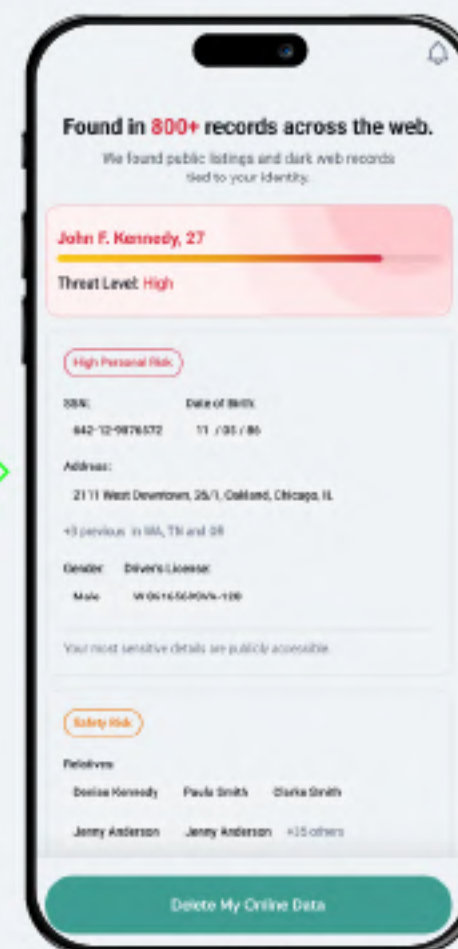
Initiate Scan



Verify Number



Initiate Scan



Scan Report

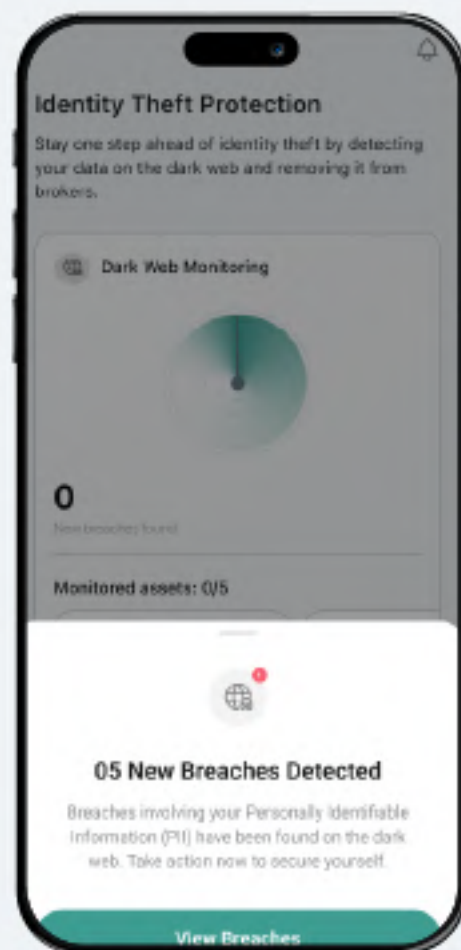
Real-Time Dark Web Monitoring

Monitor underground ecosystems to identify credential exposure, breach activity, and emerging identity threats.

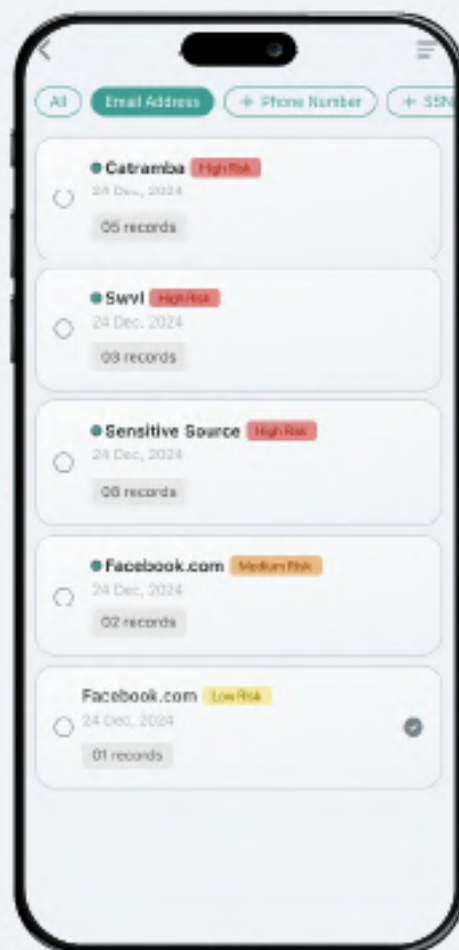


Dark Web Intelligence Engine

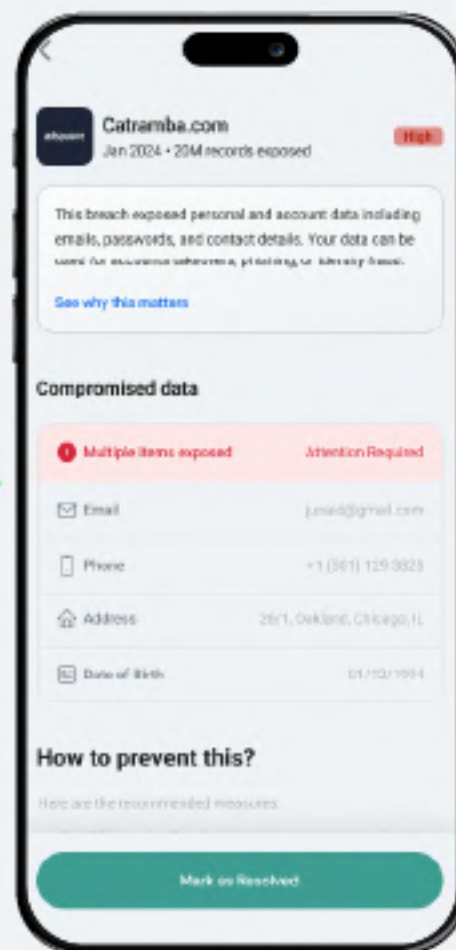
Recommended Flow



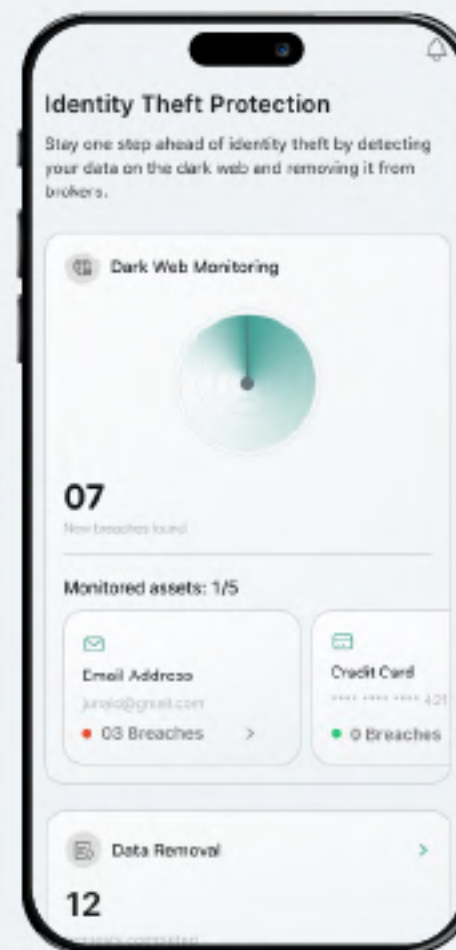
Discover Exposures



See Exposed Details



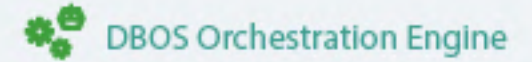
Get Remediation Steps



Enable Real-Time Monitoring

Data Broker Opt-Out Service (DBOS)

Automate privacy remediation across brokers through discovery, removal, verification, and continuous protection.



Recommended Flow

Authorize Your Data Removal

We'll submit removal requests to data brokers on your behalf.

Please review your details carefully as you won't be able to edit them later.

Email*
junaaid@gmail.com

Name*
Junaid Ahmed Siddiqui

Country*
United States

State*
Alaska

Initiate Removal

Provide Consent

Removal Requests Sent

We've officially requested your data removal from broker sites. Here's what happens next:

- Brokers process your request. Most sites take 3-14 days to remove your data. We've notified them all.
- We follow up on your behalf. If a broker delays or ignores the request, we push back automatically.
- You get notified when it's done. We'll alert you as each site confirms your data is removed.

View Dashboard

Submit Removal Request

Request Completed: 12

Time Saved: 6 days

Data removal requests will automatically resubmit every 60 days.

Filters: All, High Risk, Medium Risk, Low Risk

Broker	Status	Action
Adsquare	Completed	Not Started
Cydersoft	In Progress	Not Started
Datacenter	Pending	Not Started
Adsquare	Completed	Not Started
Adalensment	Completed	Not Started

Track Progress

adsquare.com

Marketing Records

Evidence

This page does not exist

Subscribe to our newsletter

Broker Details

Requested Status: Completed

Risk Level: 8/10

Average Response Time: 2-3 Days

Last Request Complete: 28th September

Last Removal Cycle: 28th September

Next Removal Cycle: 28th September

Type of Data Broker: Marketing Records

Get Removal Evidence

Built for OEM Scale. Designed for Simple Integration.



Plug & Play Integration

Integrate once through a unified API layer to enable exposure intelligence, dark web monitoring, remediation workflows, evidence generation, and privacy protection experiences.

→ Works across apps, portals, dashboards, and partner ecosystems.



Unified Privacy Operations

From exposure discovery and monitoring to remediation, verification, and continuous protection, the entire privacy lifecycle is orchestrated through a single platform.

→ **One integration. Multiple privacy capabilities.**



Flexible Deployment Models

Launch through APIs, white-label experiences, partner dashboards, embedded widgets, or fully managed deployments.

→ **Deploy the experience that fits your brand and business model.**

Flexible Implementation Methods

1

Full White-Label Platform Deployment

Deploy a fully branded privacy protection solution under your own brand, including exposure intelligence, dark web monitoring, remediation, evidence generation, and continuous protection.

2

Modular Capability Integration

Integrate individual privacy services independently through APIs, dashboards, embedded experiences, or partner workflows. Available Modules:

- Identity Exposure Intelligence (IEX)
- Dark Web Monitoring (DWM)
- Data Broker Opt-Out Service (DBOS).

3

Hybrid Deployment

Combine white-label experiences, APIs, and standalone modules to create a deployment model tailored to your business and customer journey.

Built for Multiple Industries and Business Models

Embedded Where Your Customers Already Are

Deploy Digital Privacy Protection across existing products, customer journeys, and partner ecosystems through APIs, white-label experiences, and modular privacy services.



Telcos & Connectivity Providers

Bundle digital privacy protection and all the module alongside existing connectivity and security services.



Cybersecurity & Privacy Providers

Expand your protection portfolio with exposure intelligence, monitoring, evidence generation, and remediation capabilities.



Financial Services & Digital Banks

Help customers reduce identity exposure risks and improve protection of personal information across digital ecosystems.



Digital Platforms & Services

Embed privacy protection directly into apps, memberships, loyalty programs, and subscription offerings.

Flexible Implementation Methods

Choose What fits Best For You

Option 1: Use our platform as a backend infrastructure layer via APIs.

Backend
Infrastructure

Partner manages client applications, user lifecycle, billing systems, and distribution channels.

Option 2: Launch quickly with ready-to-use client applications customized to your brand.

Backend
Infrastructure

Client
Applications

Partner manages user lifecycle, billing systems, and go-to-market channels.

Option 3: Take control of customer management while leveraging our infrastructure and apps.

Backend
Infrastructure

Client
Applications

User Management
System

Partner manages billing systems and distribution channels.

Option 4: Launch a complete ITP business with fully managed infrastructure, operations, and monetization.

Backend
Infrastructure

Client
Applications

User Management
System

Billing & Website

Join PureVPN Partner Program

Launch Your Digital Privacy Protection Business

Ready to launch a comprehensive Digital Privacy Protection service?

Empower consumers and businesses to discover, remediate, and continuously reduce digital privacy risks through identity exposure intelligence, dark web monitoring, data broker removal, and privacy protection services.



www.purevpn.com/white-label



support@purevpn.com



purevpn

Partner & Enterprise Solutions

Contact Information

Reach out to us for inquiries, partnership opportunities, or any questions you may have.



401, Emaar Square 1, Al Mustaqbal Street,
Burj Khaifa, Downtown Dubai.



Intershore Chambers P.O Box 4342, Road Town,
Tortola , British Virgin Islands.



info@purewl.com
support@purewl.com



www.purevpn.com/whitel-label

