Optery FOR BUSINESS

# A Security Professional's Guide to Choosing the Right Personal Data Removal Software



# Table of Contents


Foreword 3

Addressing the Problem of Data Brokers 4

Enterprise Readiness and Security Credentials 5

Self-Service Evaluation and Onboarding 6

Implementation and Expert Support 7

Search Accuracy and Demonstrated Effectiveness 8

Evidence-Based Removals 9

Real-Time Reporting and Program Visibility 10

Broad and Meaningful Data Broker Coverage 11

Frequent Scanning and Ongoing Removals 12

Transparent Pricing and Flexible Billing 13

Strong Technology Supported by Human Expertise 14

API and Security Operations Workflow Integration 15

Making the Final Decision 16


© 2026 Optery

# Foreword

## Targeted social engineering is rising, increasingly personalized and multi-channel, and straining enterprise defenses.

It is also succeeding. In Optery's 2026 Enterprise Social Engineering Survey, 96% of cybersecurity leaders reported an increase in targeted social engineering attacks, and nearly 75% said their organizations had experienced credential compromise. Respondents ranked data broker and people-search sites as the most significant source of attacker intelligence, ahead of social media and breach data.

Email security, endpoint protection, multifactor authentication, and security awareness training remain essential. However, these controls do not prevent targeted attacks from being crafted and launched in the first place. Removing exposed employee personal information helps move security upstream by reducing the intelligence threat actors can use to identify targets, map relationships, answer account-recovery questions, impersonate trusted people, and develop personalized pretexts.

This is no longer solely an executive protection concern. Attackers target people throughout an organization, including IT, finance teams, human resources, help desk staff, engineers, contractors, and executives. Publicly available PII and professional information fuels phishing, smishing, vishing, business email compromise, credential theft, account takeover, identity fraud, doxxing, harassment, and physical threats.

For organizations seeking to reduce this exposure, choosing the right personal data removal platform requires more than comparing price or counting the number of data brokers on a vendor's website. Security teams should evaluate how well a provider finds and removes personal information, how it demonstrates results, how securely it handles employee data, and how readily it fits into existing business and security operations.



**Paul Mander**
Chief Commercial Officer and General Manager, Optery for Business

# Addressing the Problem of Data Brokers

**Data brokers and people-search sites collect and publish personal information from public records, commercial sources, online activity, and other datasets.**

These sites assemble the information into detailed profiles that make it easy for attackers to conduct reconnaissance on targets.



**Removing this information manually is not feasible to scale. Every data broker has different search methods, opt-out procedures, identity-verification requirements, and response practices.**

A removal request may involve completing a form, responding to a verification email, sending a legal demand, or supplying additional information to confirm identity. Broker procedures also change, new sites emerge, and previously removed profiles may return when brokers refresh their data.

For these reasons, organizations use personal data removal platforms to scan for and remove employee PII on an ongoing basis. The following criteria can help security and privacy teams evaluate which platform will provide the most effective, secure, and manageable protection.

1

# Enterprise Readiness and Security Credentials

**Personal data removal requires the processing of sensitive employee information, so enterprise security controls are a must. A vendor should be able to support a formal security and privacy review and provide current documentation that substantiates its claims.**

Look for a recent SOC 2 Type II attestation, which evaluates whether relevant controls operated effectively over a period of time. Confirm that the platform supports secure authentication and workforce lifecycle management through capabilities such as SSO and SCIM. Buyers should also examine data encryption, access controls, retention and deletion policies, incident-response practices, subprocessors, and the availability of a Data Processing Agreement.

Enterprise readiness also includes administration. Security teams need centralized visibility, appropriate account permissions, efficient provisioning and deprovisioning, and reporting that can show exposure and removal progress across the organization.

**What to look for:**

1. A current SOC 2 Type II report and accessible compliance documentation
2. SSO and SCIM support
3. Clear data retention, deletion, encryption, and subprocessor practices
4. Centralized administration and organization-level reporting
5. Controls that support secure employee onboarding and offboarding

2

# Self-Service Evaluation and Onboarding

**Organizations should not have to complete a lengthy sales process simply to determine whether a personal data removal platform can find their employees' exposed information.**

Self-service options allow a security team to create an account, assess exposure, and understand the product before making a broader commitment.

A free scan, no-cost business account, or limited trial can also provide far more useful evidence than a generic demonstration. By testing the platform with a representative group of employees, including high-risk roles, buyers can evaluate the quality of the findings, the employee experience, the administrative workflow, and the speed with which protection can begin.

**Self-service should not mean unsupported. The strongest providers allow organizations to begin independently while preserving access to knowledgeable assistance when it is needed.**

### What to look for:

The ability to create and begin using a business account without a sales call

Free exposure scans or a trial using actual employee profiles

Clear enrollment, consent, and activation workflows

A straightforward path from initial evaluation to wider deployment

3

# Implementation and Expert Support

**Personal data removal is not a set-it-and-forget-it commodity.**

Organizations may need guidance from an expert on initial deployment, employee communications, account provisioning, interpreting reports, or complex removal cases that require additional review or specialized handling.

Evaluate whether the provider offers access to knowledgeable customer success and support personnel rather than limiting customers to automated responses or generic help content. Larger deployments may also require an implementation manager, customized onboarding materials, employee privacy training, and escalation paths for urgent or complex situations.

**The provider should be able to function as a reliable partner while still allowing the customer to manage the program efficiently through self-service tools.**

**What to look for:**

- Knowledgeable customer success and technical support
- Implementation assistance for larger deployments
- Employee onboarding resources and privacy training

4

# Search Accuracy and Demonstrated Effectiveness

**A platform cannot remove personal information it fails to find. Coverage claims therefore tell only part of the story. A vendor may list hundreds of supported sites while finding relatively few of the profiles that actually belong to a particular employee.**

Ask how the platform searches for records and matches them to the correct person. Effective discovery should account for name variations, current and former locations, aliases, related people, and other identifying details while minimizing false positives. Sophisticated matching and anti-bot capabilities are important because many data brokers actively impede automated searches.

Buyers should also look for evidence beyond the vendor's own claims. Independent evaluations, documented customer results, and a free scan or limited trial can help buyers assess how effectively a service finds and removes exposed profiles. Optery finds approximately 100 exposed profiles per person on average. This provides a useful benchmark for evaluating search breadth, while a limited trial can provide initial evidence of removal performance.

Buyers should be wary of providers that report counts of individual PII elements without disclosing the number of distinct profiles found and removed, since those larger figures do not necessarily represent broader discovery or more successful removals.

### What to look for:

1. Accurate matching across name and location variations
2. Technology designed to overcome anti-bot defenses and changing site structures
3. Low false-positive rates and clear methods for correcting mismatches
4. Independent testing, credible customer results, and third-party recognition
5. Broad discovery of exposed profiles and verifiable removal results

5

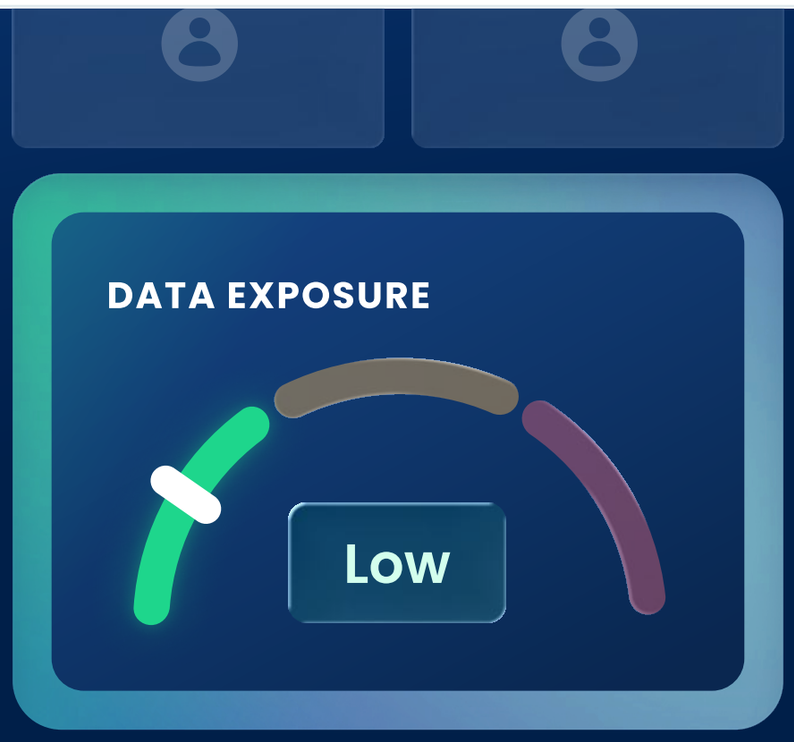
# Evidence-Based Removals

**A removal request being submitted is not the same as personal information being removed. Security teams need evidence showing what was found, what action was taken, and whether the exposed profile is no longer available.**

Look for detailed exposure reports and removals reports that include links or screenshots documenting where employee data appeared. Before-and-after screenshots provide particularly strong evidence because they allow the organization to verify the original exposure and the subsequent removal rather than relying exclusively on a vendor-generated status label.

### What to look for:

- Evidence showing where employee information was found
- Before-and-after screenshots or links verifying removal
- Clear distinctions among discovered, submitted, in-progress, and removed statuses



6

# Real-Time Reporting and Program Visibility

**Personal data removal is an ongoing process, and administrators should not have to wait for a periodic report to understand what is happening across their organization.**

A business platform should provide a live dashboard that reflects current exposure findings, removal progress, and status changes as they are recorded.

Reporting should also help administrators understand progress over time. Capabilities should include organization-level exposure and removal trends, filtering by employee, group, or status, and downloadable or exportable reports. Metrics that demonstrate PII attack surface reduction and program value can also help security teams communicate results to leadership and other stakeholders.

**Real-time reporting is separate from scanning frequency. A platform may scan employees monthly while updating its dashboard as findings are processed and removal statuses change.**

**What to look for:**

- A live administrative dashboard showing current exposure and removal progress
- Organization-level metrics and trends over time
- The ability to view or filter results by employee, group, and removal status
- Metrics that demonstrate PII attack surface reduction and program value
- Downloadable or exportable reports for analysis and stakeholder reporting

7

# Broad and Meaningful Data Broker Coverage

**There are hundreds of data brokers and people-search sites, and new sources of exposure continue to emerge. Broad coverage is essential, but headline totals can be misleading when providers count fundamentally different levels of service as “coverage.”**

Vendors should publish the exact sites automatically included under each plan and should clearly distinguish their standard automated coverage from Custom Removals for eligible sites beyond that coverage and disclose any caps or frequency limits.

A large advertised coverage number is far less meaningful when only a small portion of those sites is handled automatically and the remainder depends on limited, customer-initiated requests, or if many of the sites aren’t even data brokers.

**A comprehensive service should combine broad automated coverage with unlimited Custom Removals for eligible sites beyond its standard coverage.**

### What to look for:

1. A published, regularly updated list of the exact sites included under each plan
2. Clear counts and site lists for recurring automated scanning and removal
3. Clear separation of automated coverage and Custom Removals
4. Full disclosure of any caps or frequency limits on Custom Removals
5. Unlimited Custom Removals for eligible sites beyond standard automated coverage
6. Broad coverage of high-risk people-search and data broker sites
7. Automatic inclusion of newly supported brokers under the applicable plan

8

# Frequent Scanning and Ongoing Removals

**Personal data exposure changes and proliferates continuously. Data brokers acquire new records, update existing profiles, and republish information that was previously removed.**

Effective personal data removal therefore requires ongoing monitoring and remediation rather than a one-time cleanup.

Look for a service that performs automated scans and removals at least monthly, ideally continuously. Continuous scanning allows the platform to identify newly exposed information, verify the continuing status of earlier removals, and resubmit requests when profiles reappear.

Scan-on-demand capabilities can provide additional flexibility when an employee faces an urgent concern or needs an updated view of current exposure. Buyers should confirm that recurring scans and removals are included in the service.

### What to look for:

- Continuous automated scanning and removals
- Scan-on-demand functionality for ad hoc needs
- Recurring protection included as part of the service



9

# Transparent Pricing and Flexible Billing

**Security teams should be able to understand what a personal data removal program will cost before entering a sales process.**

Public pricing and an interactive calculator make it easy to compare coverage levels, forecast costs, and determine whether protection can be expanded to additional employees.

Look for monthly and annual billing choices, clear per-data subject or tier-based pricing, and the ability to add seats, change plans, or adjust coverage as organizational needs evolve. Organizations may also benefit from the ability to use different protection levels for different populations, such as comprehensive coverage for high-risk employees and lower-cost coverage for a broader workforce.

Be cautious of unclear pricing, unexpected add-on fees, or vendors that offer only long-term contracts.

### What to look for:

1. Publicly available pricing and the ability to calculate actual costs instantly
2. Monthly and annual billing options
3. Clear descriptions of what each plan and coverage level includes
4. Flexibility to add data subjects, change plans, or adjust coverage
5. No unnecessary long-term commitment or cancellation penalty

10

# Strong Technology Supported by Human Expertise

**The data broker ecosystem is too large and dynamic to address through manual work alone.**

Manual processes cannot search for exposed profiles and submit requests across hundreds of sites as quickly or consistently as advanced automation. Effective automation is essential for broad coverage, fast removals, and ongoing protection as personal information reappears.

Meaningful automation should extend across the removal workflow. A provider's technology should be able to locate and accurately match profiles, complete and submit opt-out forms, handle CAPTCHA challenges and other anti-bot barriers, click verification links, compose and respond to removal-related emails, deliver applicable privacy-rights and legal demands, and track requests through completion. It should also support recurring scans and repeat removals when profiles reappear.

Even advanced automation cannot resolve every case. Data broker procedures change, records can be difficult to match, and some removals require additional investigation, escalation, or specialized handling. Privacy experts should provide quality assurance, resolve exceptions, address unresponsive or noncompliant brokers, and complete eligible Custom Removals beyond standard automation.

Because service tiers may differ, buyers should determine which parts of the removal process are automated, which receive human review, and what expert assistance is included.

### What to look for:

1. Automation that searches for and accurately matches exposed profiles
2. Automated completion and submission of opt-out forms
3. Technology capable of handling CAPTCHA challenges, verification links, email correspondence, and applicable legal demands
4. Automated tracking of removal requests through completion
5. Human quality assurance and exception handling where necessary
6. Privacy experts who can address broker changes, escalations, and complex removal cases

11

# API and Security Operations Workflow Integration

**For organizations and technology partners, personal data removal may need to integrate with existing systems rather than operate solely through a standalone dashboard.**

A robust API can bring exposure and removal data into security operations or custom dashboards and embed scanning, removal, reporting, and ongoing monitoring into existing products and workflows.

Evaluate whether the API supports managing members and subscriptions; retrieving exposure statistics, data broker removal statuses, screenshots, reports, and activity history; and submitting and tracking Custom Removals and Removal Issues. Organization-level metrics and event webhooks should support automated workflows and provide timely updates on scans, opt-out submissions, reports, and other important milestones.

**Public documentation, secure authentication, and separate sandbox and production environments allow developers to evaluate and test the integration safely.**

### What to look for:

- Public API documentation, secure authentication, and separate sandbox and production environments
- API-based member and subscription management
- Access to exposure statistics, removal statuses, screenshots, reports, and activity history
- The ability to submit and track Custom Removals and Removal Issues
- Organization-level metrics for security operations and custom dashboards
- Event webhooks and support for embedding scanning, removal, reporting, and ongoing monitoring into partner products

# Making the Final Decision

### Choosing a personal data removal platform should not come down to the longest advertised broker list or the lowest quoted price.

The most effective platform will comprehensively and accurately find employee information, remove it across a broad range of sites, verify the results, repeat the work every month, and provide the security, administration, support, and integrations needed to operate at organizational scale.

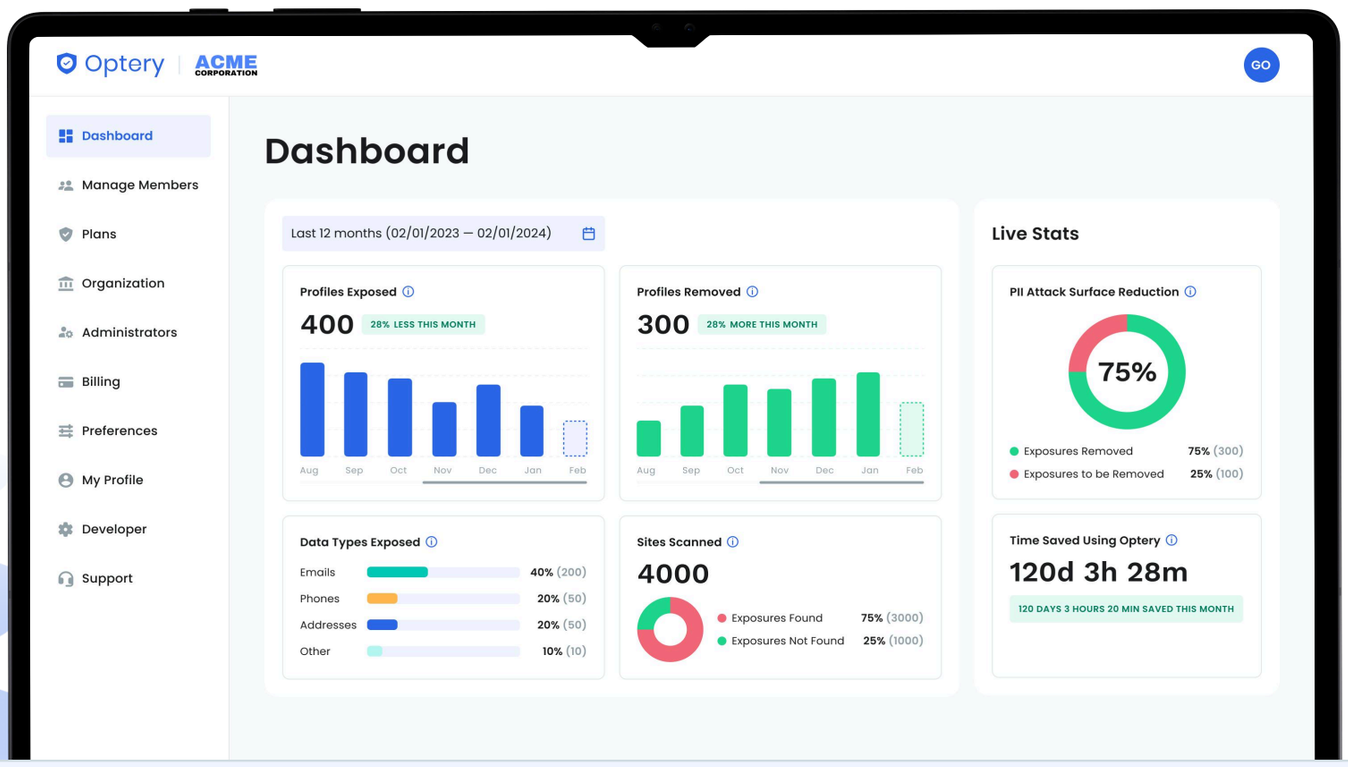
After narrowing the field using the criteria above, ask the preferred provider to offer a free 30-day trial for a select group of high-risk employees. This group might include executives and employees in IT, identity and access management, finance, human resources, and help desk functions. Evaluate the number and accuracy of exposed profiles found, the breadth of automated coverage, initial removal progress, the evidence provided, and the quality of expert support.

## Organizations already using another data removal service should also run Optery's free scan for a selection of protected employees.

Optery's patented search technology finds approximately **40 to 50 more exposed profiles** per person on average than competing services, making the free scan a direct, low-effort way to identify what an incumbent provider may have missed.

**Learn More**

**Get Your Free 30-Day Trial**




© 2026 Optery. All rights reserved.