CLUZY.

A RISK REDUCTION FRAMEWORK FOR SMALL BUSINESS

Employee Data Wellness as Cybersecurity

A Risk Reduction Framework for Small Business

Employee data wellness, self-sovereign data ownership, included People Finder website removal, and personalized additional protections reduce cyberattack threat surface and quantifiable expected loss.

Daginty / Cluzy
August 2026

01

SECTION 01

Executive Summary

Small and medium-sized businesses face a cybersecurity crisis that is simultaneously existential and poorly understood.

Approximately 50% of businesses with fewer than 100 employees report experiencing a cyberattack in any given year, and Verizon's 2025 Data Breach Investigations Report finds that 19% of breached small businesses report the incident contributed to bankruptcy.[1] The average direct cost of a single SMB breach exceeds $250,000 - a figure that, combined with reputational damage, regulatory exposure, and operational disruption, can threaten the survival of under-capitalized organizations. Yet the security products designed to address this threat have been built almost entirely for enterprise IT environments: costly, complex, and dependent on dedicated security personnel that most small businesses simply do not have.

The market gap is not technological. It is human. The Verizon 2025 Data Breach Investigations Report finds that the human element is involved in 60% of all breaches[1] - through phishing, social engineering, credential theft, and misuse. Existing solutions respond to this finding with annual compliance training: static, click-through modules that employees complete to satisfy an audit requirement rather than to genuinely change behavior.

Cluzy is built on a different thesis: that an employee's data wellness is the most effective, most scalable, and most measurable intervention available to SMBs today. This whitepaper presents three strategic pillars that define the Cluzy model:

Three strategic pillars

The Self-sovereign Data Stipend

Employers pay employees up to $250* per year as a financial incentive to build and maintain a verified, self-reported self-sovereign data profile - transforming a privacy product into a financial wellness benefit.

Included Removal + Employee Choice

The updated experience begins with a guided Google Takeout DSAR action. Cluzy then furnishes an included People Finder website removal service through its primary provider, with verified coverage across 300+ data brokers and an always-current coverage list. This baseline targets the identity, relationship, address, and phone data that makes phishing emails and vishing calls credible. Cluzy also presents personalized options for additional protection, and the employee decides whether to add them.

Dual TSRI Metrics

The Threat Surface Reduction Index now tracks two leading indicators that drive enterprise cybersecurity risk reduction: number of self-sovereign profiles created and number of employees enrolled in a deletion service. For dashboard purposes, the deletion-side leading indicator is now reported as Number of Employees Who Have Taken Deletion Action, beginning with the Google Takeout DSAR checkpoint.

ILLUSTRATIVE OUTCOME

19.2x return on investment

Using conservative parameters grounded in published industry data, a fully engaged 100-person company can protect an estimated $307,800 per year of enterprise value against an annual platform cost of $16,000 - a 19.2x return on investment.

Even at 25% participation, protected value exceeds program cost by more than four times. These figures transform Cluzy from a wellness benefit into a financially defensible risk mitigation instrument, directly comparable to cybersecurity insurance - and because Cluzy functions like an insurance policy against the human-element breach vector, customers have a credible basis to negotiate lower cybersecurity insurance premiums with their carrier as a result of adopting it.

02

SECTION 02

The SMB Cybersecurity Crisis

The scale of the cybersecurity threat facing small businesses is not fully appreciated by mainstream discourse, which tends to focus on headline-generating enterprise breaches.

2.1 - Scale of the Problem

Industry survey data consistently shows that approximately 50% of small businesses with 100 or fewer employees report being the target of a cyberattack in any given 12-month period.[1] Unlike large corporations, which possess legal, technical, and financial resources to absorb and recover from breaches, small businesses typically lack all three. Verizon’s 2025 Data Breach Investigations Report finds that 19% of small businesses suffering a breach report the incident contributed to bankruptcy.[1] The average per-incident cost - including direct remediation, legal exposure, lost productivity, customer

notification, and reputational damage - is approximately $250,000.

The proximate cause of the majority of these breaches is not technological vulnerability but human behavior. The Verizon 2025 DBIR finds that the human element is implicated in 60% of all breaches[1,2], encompassing phishing, pretexting, social engineering, and the misuse of legitimate credentials. Within the broader human-element category, 22% of breaches were initiated through credential abuse and 16% through phishing attacks.[3]

2.2 - The Data Broker Threat Vector

A structural feature of the modern cyberattack ecosystem that receives insufficient attention in SMB security discourse is the role of commercial data brokers as attack infrastructure. Broker firms aggregate, package, and sell detailed personal records on hundreds of millions of individuals. A typical broker record contains: full legal name, current and historical addresses, email addresses, phone numbers, employer and work location, marital and family status, purchase history, and online activity patterns.[4] This is precisely the information required to construct a credible, personalized phishing email or vishing call.

The global data broker market was valued at approximately $257 billion in 2023 and is projected to reach $561 billion by 2029, growing at 7.4% annually.[5] Conservative modeling suggests broker-held employee data is implicated in approximately 30% of human-element attacks on small businesses - the basis of the Cluzy risk quantification model in Section 4.

2.3 - Why Data Deletion Alone Is Security Theater

The conventional response to broker data exposure has been deletion services: automated opt-out tools that submit removal requests to broker databases on an employee's behalf. The privacy industry markets these services as meaningful protection. The evidence tells a more complex story.

- Data re-aggregates. Brokers pull from source records - public records, purchase data, credit headers - on rolling cycles. Research from DeleteMe's own operations shows data re-appears within 3-6 months on average. Opt-out suppresses a copy; it does not destroy the source.
- Opt-out confirms the record. The deletion process requires submitting name, address, and sometimes government ID to prove identity. The employee provides more verified PII to the broker than the broker held before.
- Scale is unachievable. Leading deletion services cover 40-50 brokers. There are 4,000+ data brokers operating in the United States. The brokers that matter most to advertisers, insurers, and attackers are rarely on opt-out lists.
- Opt-out lists get monetized. There is documented evidence of suppression lists being treated as high-value targeting segments - someone who cared enough to opt out is a motivated, privacy-aware consumer.

As of August 1, 2026, California's Delete Request and Opt-out Platform (DROP) gives state residents a free, state-run mechanism to submit a single deletion request to the 500+ data brokers registered with the California Privacy Protection Agency; registered brokers must honor a verified request within 90 days.[13] This is a genuine regulatory milestone, and it validates the core thesis of this whitepaper - broker-held personal data is a material, recognized cyberattack threat vector, serious enough to warrant a dedicated state deletion infrastructure. It does not, however, close the gaps above: DROP only reaches brokers meeting California's statutory registration threshold, processes a one-time request rather than monitoring for re-appearance, and produces no verification or reporting layer an employer, insurer, or board member can rely on.

The strategic implication is important: Cluzy furnishes every participating employee with an included People Finder website removal service, delivered through its primary provider across 300+ data brokers with an always-current coverage list. People Finder websites expose the identity, relationship, address, and phone data that social engineers use to personalize phishing emails and vishing calls, making this included service the most direct deletion response to the primary threat vector. Cluzy then presents options for additional protection based on the specific data types found in the employee's broker record. The employee decides whether they want protection beyond the included People Finder website removal service. An optional AI advisor can explain the differences among matched services and why each may fit the employee's exposure, but Cluzy does not choose or enroll on the employee's behalf. The core value proposition remains diagnosis, self-sovereign ownership, employee agency, and measurable risk reduction.

2.3a - Cluzy's Layered Deletion Response

Cluzy operationalizes that strategy in three layers. First, Cluzy walks each employee through a Google Takeout DSAR workflow, supported by an AI agent and/or tutorial video, so the employee can complete a concrete deletion action. Second, Cluzy furnishes an included People Finder website removal service through its primary provider, which continuously handles removals across 300+ data brokers and keeps its coverage current. This included layer reduces the public identity and contact data used to make phishing and vishing attacks credible. Third, Cluzy diagnoses the employee's remaining exposure and presents one or two additional protection options suited to those data types. The employee decides whether to add them, with an optional AI advisor available to explain the recommendations.

2.4 - The Failure of Traditional Cybersecurity Training

Compliance-driven training fails because it does not engage the employee as a stakeholder with a personal interest in the outcome. Retention of training content delivered in a single session decays rapidly; research on distributed practice shows that spacing and reinforcement improve long-term retention compared with a single massed session.[14] More fundamentally, an employee completing a mandatory module understands that the beneficiary of their compliance is the organization - not themselves. There is no moment of personal recognition that their own data is exposed, that their family's information is for sale, or that the phishing email they are being trained to resist will be crafted using information bought from a data broker.

03

SECTION 03

The Cluzy Framework: Employee Data Wellness as Cybersecurity

Data security protects the perimeter. Employee data wellness strengthens the people inside it - and gives them ownership of the personal information that attackers exploit.

3.1 - Conceptual Foundation

‘Data security’ in the conventional IT sense is a defensive, perimeter-oriented posture: firewalls, access controls, endpoint detection, and incident response. It treats the human employee as a liability to be managed. ‘Employee data wellness,’ by contrast, is a proactive, human-centric orientation. It starts from the premise that employees have their own data identities - personal records held by hundreds of brokers, behavioral signals generated by daily digital activity, and privacy habits that either protect or expose them and their employer.

The foundational philosophy of the Cluzy platform:

> *Every business needs two things: People and Data. If you want a strong business, you must protect and empower your people and protect your data. Data security starts with data privacy.*

3.2 - The Data Wellness Score (DWS)

The Data Wellness Score (DWS) converts discrete employee actions - each with a documented relationship to threat surface reduction - into a normalized 0-100 score. The score is gamified and visible to the employee, creating intrinsic motivation and enabling peer benchmarking.

DWS actions

Action	Points	Rationale
Self-sovereign profile created	20	Verified self-reported data established; foundation of the data economy exit
Google Takeout DSAR completed	Aware checkpoint (minimum DWS 26)	Checks the deletion-action box and advances the employee from Unprotected to at least the Aware tier
Data broker record removed	10	Direct elimination of a spear-phishing vector
Deletion service enrolled	10	Sustained suppression of broker re-aggregation
Broker opt-out submitted	5	Proactive suppression of future data collection
Data Wellness module completed	3	Behavioral change - the human layer
Privacy hygiene check completed	3	Credential and identity exposure reduction
Data Genius milestone reached	25 (one-time)	Full program completion - comprehensive protection

DWS scores classify into four protection tiers: Unprotected (0-25), Aware (26-50), Protected (51-75), and Data Genius (76-100). Note that self-sovereign profile creation and deletion service enrollment now carry elevated point values, reflecting their disproportionate impact on organizational threat surface. Completing the guided Google Takeout DSAR marks the deletion-action checkpoint and sets the employee's DWS to at least 26, moving them above Unprotected into the Aware tier.

3.3 - The Threat Surface Reduction Index (TSRI)

The TSRI translates individual DWS tier classifications into a quantified estimate of reduced breach probability. The methodology is grounded in three empirical anchors: (1) Verizon's finding that 60% of breaches involve the human element [1]; (2) the conservative industry estimate that approximately 30% of human-element attacks on SMBs rely on broker-sourced data; and (3) the plausible reduction in susceptibility associated with each DWS engagement level.

Threat Surface Reduction Index

DWS tier	TSRI (Threat Surface Reduction)
Unprotected (0-25)	0%
Aware (26-50)	15%
Protected (51-75)	35%
Data Genius (76-100)	60%

The company-level TSRI is the headcount-weighted average of individual employee TSRIs, updated in real time as DWS scores change. The 60% ceiling is intentionally conservative - it does not claim that broker removal eliminates all phishing susceptibility, only the broker-sourced component of social engineering targeting.

3.3a - The Two Leading TSRI Indicators

The TSRI is driven by two measurable leading indicators that give employers concrete, trackable milestones: self-sovereign profiles created and Number of Employees Who Have Taken Deletion Action. Deletion service enrollment remains a supporting operational submetric.

Leading TSRI indicators and supporting deletion metric

Indicator	What It Measures	Why It Matters
Self-sovereign Profiles Created	Number of employees with an active, verified zero-party data profile	Each self-sovereign profile represents an employee who has exited the broker data economy as a passive subject and entered it as an active, compensated participant. Profiles drive TSRI by replacing exploitable guessed data with verified, consent-gated data that attackers cannot access.
Number of Employees Who Have Taken Deletion Action	Number of employees who have completed the guided Google Takeout DSAR and checked the DWS deletion-action box	This is the primary deletion-side dashboard indicator. It records a concrete employee action, advances the employee to at least the Aware tier, and creates a consistent milestone that can be measured across the workforce.
Deletion Service Enrollments	Number of employees covered by the included People Finder website removal service or enrolled in an employee-selected additional service	Deletion alone is not sufficient, but sustained deletion service engagement meaningfully reduces the volume of broker data available for targeting. The included service focuses on People Finder websites used for phishing and vishing reconnaissance; additional services deepen or broaden coverage based on the employee's diagnosed exposure. This remains visible as a supporting breakdown beneath the primary deletion-action indicator.

These two indicators serve as the primary dashboard KPIs reported to employers, insurers, and board members. An employer can track week-over-week progress in both dimensions and model the expected TSRI impact of each additional profile or enrollment. The dashboard label for the deletion dimension is Number of Employees Who Have Taken Deletion Action; provider enrollment is retained as a supporting operational measure.

3.4 - The Personal Data Value (PDV) Score

The PDV Score quantifies the estimated economic value of the self-sovereign data profile each Cluzy user has built - the data they have actively contributed, verified, and consent-gated through the platform. PDV reflects what the profile is worth, not a claim about what has been removed from broker databases. (A consent-gated licensing program to vetted brand partners is a roadmap consideration and is not part of the initial Cluzy product release.)

The PDV is composed of three analytically distinct inputs:

PDV inputs

Input	Description	Modeled Value or Factor
Behavioral Signal Value (BSV)	Value of consensual zero-party / first-party data generated through active Cluzy platform use.[7]	$300-$500
Data Wellness Score Factor (DWS%)	The employee's current DWS engagement and profile-completeness level, expressed as a percentage, that scales BSV.	0%-100% scaling factor
Self-sovereign Data Premium (SDP)	1.2-1.5x multiplier for data carrying documented consent, verifiable audit trail, and zero broker contamination - valued in regulated industries.[8]	1.2-1.5x multiplier

01 PDV = (BSV × DWS%) × SDP multiplier

PDV grows as employees engage more deeply with the platform - creating a continuous incentive for progression through DWS tiers.

3.5 - The Self-sovereign Data Stipend

Employers pay employees up to $250*/year to build and maintain a self-sovereign data profile. The data economy has been extracting value from employees without compensation for decades. Cluzy reverses that.

The Self-sovereign Data Stipend is Cluzy's most significant strategic departure from the deletion-first model that dominates the privacy services market. Rather than asking employees to opt out of the data economy - a largely futile exercise demonstrated in Section 2.3 - Cluzy invites employees to opt in to a better version of it, on their own terms and for their own financial benefit.

THE STIPEND

Up to $250 per employee, per year

Employers fund a flexible benefit that rewards employees for building and maintaining a self-sovereign data profile.

How the Stipend Works

Stage	Description
Employer Funds Stipend	The employer allocates up to $250* per employee per year as a wellness benefit - comparable in structure and tax treatment to an HSA contribution or a gym membership benefit.
Employee Builds Self-sovereign Profile	The employee uses Cluzy to build a verified zero-party data profile: behaviors, interests, preferences, motivations, and feelings - confirmed by the individual, not inferred. Each completion threshold unlocks the next stipend tier.
Profile Generates Licensed Revenue	With explicit, granular consent, the self-sovereign profile is made available to vetted brand partners - financial services, healthcare, consumer brands - who pay a premium for verified first-party data. The employee receives a share of this revenue.
Stipend + Revenue Share = $250* Target	The employer-funded stipend seeds the benefit; licensed data revenue supplements it. The $250* target represents the combined annual value delivered to the employee for maintaining an active self-sovereign profile.
Benefit Delivery Format	The $250* is not required to be cash. The employer determines and administers how the benefit is delivered - through their own HR and payroll systems. Delivery formats may include Money (direct payroll or deposit), Recognition (awards, public acknowledgment), Time Off (additional PTO or flex days), or a custom benefit the employer defines. Cluzy does not prescribe or facilitate delivery; the employer is solely responsible for making the benefit available.

Why $250* Works

The deletion services market has demonstrated that people will not opt out of data brokers for privacy reasons in meaningful numbers - consumer motivation for abstract privacy protection is low. People will, however, take concrete action for a concrete financial reward. The $250* stipend structure solves the adoption problem that has historically limited privacy product engagement to a small, already privacy-motivated minority.

The $250* framing also positions the stipend correctly within enterprise HR budgets. ‘$250* data wellness benefit’ fits alongside fitness reimbursement, mental health apps, and financial planning tools - benefits that HR teams already champion and CFOs already approve. It avoids the procurement friction of a new cybersecurity line item while delivering a cybersecurity outcome.

Critically, the $250* does not have to be delivered as cash. The employer determines how the benefit is administered through their own HR and payroll systems. Delivery formats include Money (direct payroll addition or deposit), Recognition (formal acknowledgment or awards), Time Off (additional PTO or flexible scheduling), or a custom benefit the employer defines. Cluzy does not prescribe or facilitate delivery - the employer is solely responsible for making all benefit options available to employees. This means the stipend can be structured to fit within existing HR systems - as a wellness benefit, a recognition program, or a cash equivalent - without requiring new payroll infrastructure or board approval for a new budget category.

* Cluzy recommended starting amount; the employer may choose to offer more.

The Competitive Implication

Deletion services sell fear and deliver theater. Cluzy sells financial agency and delivers a measurable, self-sovereign data asset. The employee is not a passive subject of the data economy - they are a compensated participant in a better version of it

that they control. This distinction is fundamental to Cluzy's brand, its user engagement model, and its long-term defensibility against deletion-first competitors.

Cluzy also functions economically like an insurance policy: it continuously reduces the human-element attack surface that drives the majority of SMB breaches. Because the DWS and TSRI metrics give employers an auditable, ongoing record of that risk reduction, Cluzy customers have a reasonable basis to raise the point with their cybersecurity insurance carrier and negotiate a lower premium - turning a wellness benefit into a line item with a second, independent source of return.

Additional Protection Marketplace Categories

Optional Protection Category	Best For	Illustrative Additional Options
Broad Consumer Deletion	General opt-out coverage across the most common brokers	DeleteMe, Kanary, Incogni (Surfshark), Optery
People-Search Expansion	Extending beyond Cluzy's included People Finder website removal coverage	OneRep, Removaly, BrandYourself
Financial & Credit Data	Data affecting lending, insurance, employment screening	Privacy Bee, DataSeal; direct opt-outs for ChexSystems, LexisNexis
Digital Footprint / Account Deletion	Closing old accounts, removing social traces, app permissions	Jumbo Privacy, Account Killer, Just Delete Me
Legal / DSAR Specialists	Formal data subject access requests with legal-weight deletion	Mine (mine.legal), Transcend, Persona
Dark Web Monitoring Add-ons	Active misuse monitoring and breach response	Mozilla Monitor, Aura, IDX

Marketplace matching logic: after furnishing the included People Finder website removal service, Cluzy diagnoses the specific data types present in each employee’s broker record, then surfaces the 1-2 additional deletion services best suited to those data types. An employee with heavy geographic precision data and people-search exposure receives a different recommendation than one whose primary exposure is financial and credit data. This personalization increases conversion, improves outcomes, and demonstrates Cluzy’s diagnostic depth. Cluzy presents the recommendations and explains the match; the employee decides whether they want protection beyond the included service. An optional AI advisor can answer questions, compare coverage, and help the employee make that decision without choosing or enrolling on the employee’s behalf.

3.6 - The Three-Layer Deletion Experience

The updated Cluzy deletion experience converts an abstract privacy recommendation into a guided action path with a clear starting point, included People Finder website coverage, and employee-selected optional expansion.

How deletion works in Cluzy

Layer	Employee Experience	Program Role
1. Guided Google Takeout DSAR	Cluzy walks the employee through a Google Takeout DSAR request with an AI agent and/or tutorial video and helps the employee file it.	Completing the task checks the DWS deletion-action box, sets DWS to at least 26 (Aware), and increments Number of Employees Who Have Taken Deletion Action.
2. Included People Finder Website Removal	Cluzy furnishes an included People Finder website removal service through its primary provider, covering removals across 300+ data brokers with an always-current coverage list.	Targets the public identity, relationship, address, and phone data used to personalize phishing emails and vishing calls.
3. Employee-Selected Additional Protection	Cluzy diagnoses the employee's remaining exposure and presents the 1-2 additional deletion services best suited to those data types. An optional AI advisor can explain and compare the recommendations.	The employee decides whether to add protection beyond the included People Finder service; Cluzy does not choose or enroll on the employee's behalf.

For dashboard purposes, the first completed layer is the consistent leading milestone: Number of Employees Who Have Taken Deletion Action. The dashboard can then show included-provider and optional-partner enrollments as supporting measures that explain the depth and continuity of each employee’s deletion coverage.

04

SECTION 04

The Existential Risk Buy-Down Model

The model asks the question that matters to an owner: what is the probability that a cyberattack becomes a business-ending event, and how much can that probability be reduced?

4.1 - Foundational Framework: Existential Risk Buy-Down

The Expected Loss Reduction Model is grounded in a risk buy-down and annual loss expectancy framework, a standard methodology in enterprise cyber and actuarial risk quantification.[9,10] Rather than modeling breach cost as a per-employee multiplier - which conflates headcount with financial exposure - the model treats headcount-driven human risk as a driver of probability, not of cost magnitude. The relevant question for an SMB owner is not ‘what does an average breach cost,’ but ‘what is the probability that a breach becomes an existential, business-ending event, and how much can that probability be reduced.’

The model combines two probabilities: the Annual Rate of Occurrence (ARO, the likelihood of experiencing a cyberattack in a given year) and the Existential Risk Rate (ERR, the likelihood that a breach, once it occurs, contributes to business

bankruptcy). The product of these two terms is the Baseline Existential Risk - the unconditional annual probability that an unprotected SMB suffers a bankruptcy-triggering event. The Threat Surface Reduction Index (TSRI, Section 3.3) then reduces that probability in proportion to employee engagement, and the resulting reduction in probability is priced against the enterprise's value at stake.

By adopting this framework, Cluzy positions its value proposition in the same analytical language that CFOs, risk managers, and underwriters already use - enabling direct comparison between the cost of the program and the enterprise value it protects.

4.2 - Baseline Existential Risk for a 100-Person SMB

Illustrative 100-person SMB

Parameter	Value	Source
Headcount	100 employees	Illustrative SMB
Annual revenue (illustrative)	$20,000,000	SMB revenue-per-employee benchmark[11]
Enterprise value at stake (1.5x revenue)	$30,000,000	Computed
Annual probability of attack (ARO)	50%	Industry surveys
Existential Risk Rate (ERR) - breach contributes to bankruptcy	19%	Verizon DBIR 2025
Baseline Existential Risk (ARO x ERR)	9.5%	Computed
Human-element fraction	60%	Verizon DBIR 2025
Broker-data contribution to human-element attacks	30%	Conservative estimate
Cluzy-addressable share (60% x 30%)	18%	Computed

Illustrative company sized at $200K revenue per employee, consistent with published SMB benchmarks; enterprise value estimated at 1.5x annual revenue, within typical small-business valuation ranges.[11,12]

This model uses a $20 million-revenue, 100-person company as an illustrative SMB - consistent with published revenue-per-employee benchmarks for firms of this size.[11] Enterprise value is estimated at 1.5x annual revenue, within published small-business valuation ranges.[12] These figures are held fixed in this whitepaper; our companion interactive ROI calculator allows underwriters and prospective customers to adjust revenue, headcount, the enterprise value multiple, risk tolerance and other factors directly.

4.3 - Applying TSRI to Derive Protected Enterprise Value

01 **Adjusted Existential Risk = Baseline Existential Risk x (1 - Company-Level TSRI)**

02 **Value Protected = Enterprise Value x Risk Reduction x Cluzy-Addressable Share (18%)**

Protected enterprise value

Participation Rate	Avg Company TSRI	Adjusted Existential Risk	Value Protected	Annual Cluzy Cost	ROI
Baseline	0%	9.50%	$0	$16,000	-
25%	15%	8.08%	$76,950	$16,000	4.8x
50%	30%	6.65%	$153,900	$16,000	9.6x
75%	45%	5.23%	$230,850	$16,000	14.4x
100% (Data Genius)	60%	3.80%	$307,800	$16,000	19.2x

These ROI figures are not marketing projections - they are the output of a conservative, auditable model using published inputs and the same addressable-risk discipline applied throughout Section 4. At zero engagement, Cluzy has reduced no risk and claims no value - the model is constructed so protected value scales directly and only with actual employee participation. Even the 25%-participation scenario returns more than four times the program cost. At full Data Genius engagement, the ROI exceeds 19x, while the underlying existential risk facing the business falls by 60% in relative terms - from a 9.5% to a 3.8% annual probability of a bankruptcy-triggering event.

4.4 - TSRI Impact of the Two Leading Indicators

The two leading indicators - self-sovereign profiles created and deletion service enrollments - drive TSRI directly. Under the updated operating model, the employer dashboard reports the deletion-side indicator as Number of Employees Who Have Taken Deletion Action, while provider enrollment remains a supporting measure. The table below models the incremental TSRI impact of each indicator at scale for a 100-person company:

Impact of the two leading indicators

Scenario	Profiles Created	Deletion Enrollments	Est. Company TSRI	Est. Value Protected
Baseline (no engagement)	0	0	0%	$0
Early awareness	20	10	8%	$41,040
Active program	60	40	28%	$143,640

Scenario	Profiles Created	Deletion Enrollments	Est. Company TSRI	Est. Value Protected
Full engagement	100	75	52%	$266,760
Data Genius (all)	100	100	60%	$307,800

4.5 - Dashboard: Real-Time Value Visibility

The real-time employer dashboard surfaces six core metrics continuously. These are not vanity metrics - each directly feeds the Value Protected calculation and can be reported to insurance underwriters, board members, and investors as evidence of active risk management. The updated dashboard adds the deletion-action milestone as the primary deletion-side indicator and retains provider enrollment as a supporting measure:

Dashboard metrics

Metric	What It Represents
Self-sovereign Profiles Created	Count of employees with active zero-party data profiles - the primary new leading TSRI indicator.
Number of Employees Who Have Taken Deletion Action	Count of employees who completed the Google Takeout DSAR workflow and checked the DWS deletion-action box - the primary deletion-side leading indicator.
Deletion Service Enrollments	Count of employees covered by the included People Finder website removal service or enrolled in an employee-selected additional service - a supporting measure of deletion coverage depth and continuity.
Participation Rate	Percentage of enrolled employees actively engaging with Cluzy activities.
Average Company TSRI	Headcount-weighted mean of individual TSRIs - the single risk posture number for underwriters and CFOs.
Value Protected (Annualized)	Company TSRI applied to Cluzy-addressable existential risk, priced against enterprise value, in real-time dollars.
Protected Data Value	Aggregate estimated value of self-sovereign data profiles created by Cluzy users - what those profiles are worth, based on the data employees have actively contributed and verified through the platform.

05

SECTION 05

Pilot Program Design

A 90-day pilot is structured to minimize procurement friction while producing enough engagement data to validate the Expected Loss Reduction model.

5.1 - Pricing and Structure

The Cluzy pilot is structured to minimize procurement friction for SMB decision-makers while delivering sufficient engagement data to validate the Expected Loss Reduction model. The pilot runs for three months at $40 per employee - a per-seat cost low enough to be approved at the operational budget level without board involvement in most small businesses. For a 100-person company, the total pilot investment is $4,000. Ongoing subscription pricing converts to $13.33 per employee per month, or $160 per employee per year.

The Self-sovereign Data Stipend ($250*/year) is funded separately by the employer as a benefit line item - not included in the platform subscription cost. Stipend funding is seeded by the employer and supplemented by licensed data revenue share as employees build active self-sovereign profiles.

Commercial structure

$40 per employee Three-month pilot price. A 100-person pilot totals $4,000.	**$160 per employee** Annual platform subscription after the pilot.
Up to $250 benefit Separately funded by the employer and not included in platform pricing.	

5.2 - Target Customer Profile

Cluzy is initially targeted at organizations with fewer than 500 employees that do not employ a dedicated CISO or CDO. The typical decision-maker is the Owner/CEO or COO - not an IT department head. The Expected Loss Reduction model is designed to speak directly to this audience: it converts a technical cybersecurity problem into a financial risk management question that any business owner can evaluate using familiar cost-benefit logic.

5.3 - Go-to-Market via Benefits Brokers

Cluzy's primary go-to-market channel is the benefits brokers owned by the country's largest insurance companies - that already hold trusted relationships with SMB owners in major metropolitan markets. These firms are uniquely positioned to

introduce Cluzy as an employee data wellness layer that complements their existing HR-sponsored benefits and total rewards programs. Broker partners receive a differentiated offering that strengthens client relationships, a concrete risk reduction narrative that supports their own value proposition, and a benefit employees immediately understand alongside the health and retirement programs those brokers already administer.

5.4 - Investor-as-Lead Insight

Startup companies are among the most vulnerable organizations to social engineering and targeted phishing - founders, executives, and early employees are high-value targets whose personal data is extensively indexed in broker databases. Cluzy's investor-as-lead channel leverages this reality: impact investors who fund Cluzy portfolio companies can introduce Cluzy as a standard operating practice across their portfolio, creating an institutional distribution channel that operates independently of the channel partner network.

5.5 - Pilot Success Metrics

Pilot engagements are evaluated against the following KPIs, reported to the employer at the close of the 90-day pilot period:

90-day pilot success metrics

Metric	Target	Rationale
Self-sovereign Profiles Created	Target 40% of enrolled employees	Primary TSRI leading indicator
Number of Employees Who Have Taken Deletion Action	Tracked for every enrolled employee	Primary deletion-side dashboard indicator
Deletion Service Enrollments	Target 30% of enrolled employees	Supporting measure of sustained deletion coverage
Average DWS Score	Target 45 (Aware tier)	Baseline engagement achievement
Company TSRI	Target 15%	Minimum threshold for meaningful ELR demonstration
Expected Loss Avoided	Target 5x pilot cost	ROI threshold for renewal recommendation

06

SECTION 06

Conclusion

The convergence of data privacy, employee wellness, self-sovereign data ownership, and cybersecurity risk management is not coincidental.

It reflects a structural truth about where breaches originate: not from unpatched servers or misconfigured firewalls, but from the personal data of real people that has been aggregated, packaged, and sold to anyone willing to pay for it.

The Cluzy model presented in this paper addresses that structural truth through three interlocking pillars. The Self-sovereign Data Stipend transforms privacy into a financial wellness benefit - solving the consumer motivation problem that has historically limited privacy program participation to an already-motivated minority. The Data Deletion Marketplace positions Cluzy as a trusted diagnostic guide rather than a single-vendor solution, improving both trust and referral revenue. And the dual TSRI indicators - self-sovereign profiles created and deletion service enrollments - give employers, insurers, and board members two concrete, trackable metrics that translate human behavioral change into quantified, auditable risk reduction. Operationally, the deletion path begins with a guided Google Takeout DSAR and continues with an included People Finder website removal service furnished by Cluzy through its primary provider, with verified coverage across 300+ data brokers. Cluzy then diagnoses the employee's remaining exposure and presents one or two matched options for additional protection; the employee decides whether to add them, with optional AI guidance available. For dashboard purposes, Number of Employees Who Have Taken Deletion Action is the primary deletion-side indicator, with service coverage and additional enrollment retained as supporting measures.

Cluzy occupies a position that no current vendor holds. DeleteMe and its peers sell suppression. Cluzy sells self-sovereignty. The employee is not a passive subject of the data economy - they are a compensated participant in a better version of it that they control. The employer is not buying a privacy tool - they are buying a measurable reduction in the probability of a breach that could cost them orders of magnitude more than the program itself.

The SMB cybersecurity market is underserved, the regulatory tailwind is strengthening, and the data broker economy is under increasing scrutiny from regulators, plaintiffs, and the public. Cluzy's timing is not coincidental - it is the product of a structural market convergence that creates a narrow window for a first-mover to establish the self-sovereign data standard for the SMB security market for the remainder of this decade. We welcome the conversation.

SOURCES

References

1. Verizon 2025 Data Breach Investigations Report
2. Mimecast: Verizon - 60% of Breaches Involve Human Error
3. Beyond Identity: Verizon DBIR 2025 - Access is Still the Point of Failure
4. Barracuda Networks: How data brokers affect the threat ecosystem
5. Cloaked: The Data-Broker Economy Will Hit $561B by 2029
7. Datapods: What your data is actually worth
8. CNIL: Monetization of personal data - how much is our data worth
9. UpGuard: What is Cyber Risk Quantification
10. Lean Compliance: Cybersecurity Risk - An Overview of Annual Loss Expectancy
11. HRBench: Revenue Per Employee
12. Phoenix Strategy Group: Valuation Multiples for Small Businesses
13. California Privacy Protection Agency: Delete Request and Opt-out Platform (DROP)
14. Cepeda et al.: Distributed practice in verbal recall tasks - a review and quantitative synthesis
15. NIST: Building Your Small Business' Cybersecurity Team - From In-House to Outsourcing