

Optery for Financial Services

Verifiable Reduction of Employee PII Exposure



The Risk

Financial Services remains one of the **most targeted sectors** in the U.S.

⚠️ In 2025, the average cost of a data breach in the financial services sector reached \$5.56 million.

⚠️ Phishing, smishing, and BEC remained the #1 breach root cause

Threat actors conduct reconnaissance before launching attacks. Data broker and people-search sites expose employee and executive data that can be used to target institutions with phishing, smishing, vishing, impersonation, account takeover, fraud, doxing, and physical threats.

Optery's Role

Optery transforms exposed employee PII from an unmanaged risk into a **continuously enforced security control**.

We identify and remove exposed employee and executive personal data across hundreds of data broker and people-search sites, disrupting attacker reconnaissance and targeting.

How We Help Financial Services Organizations

High-Risk Employee Exposure Reduction

Remove exposed contact details and other personal data used to target executives, long-term employees, and other high-risk staff.

Continuous Exposure Monitoring and Removal

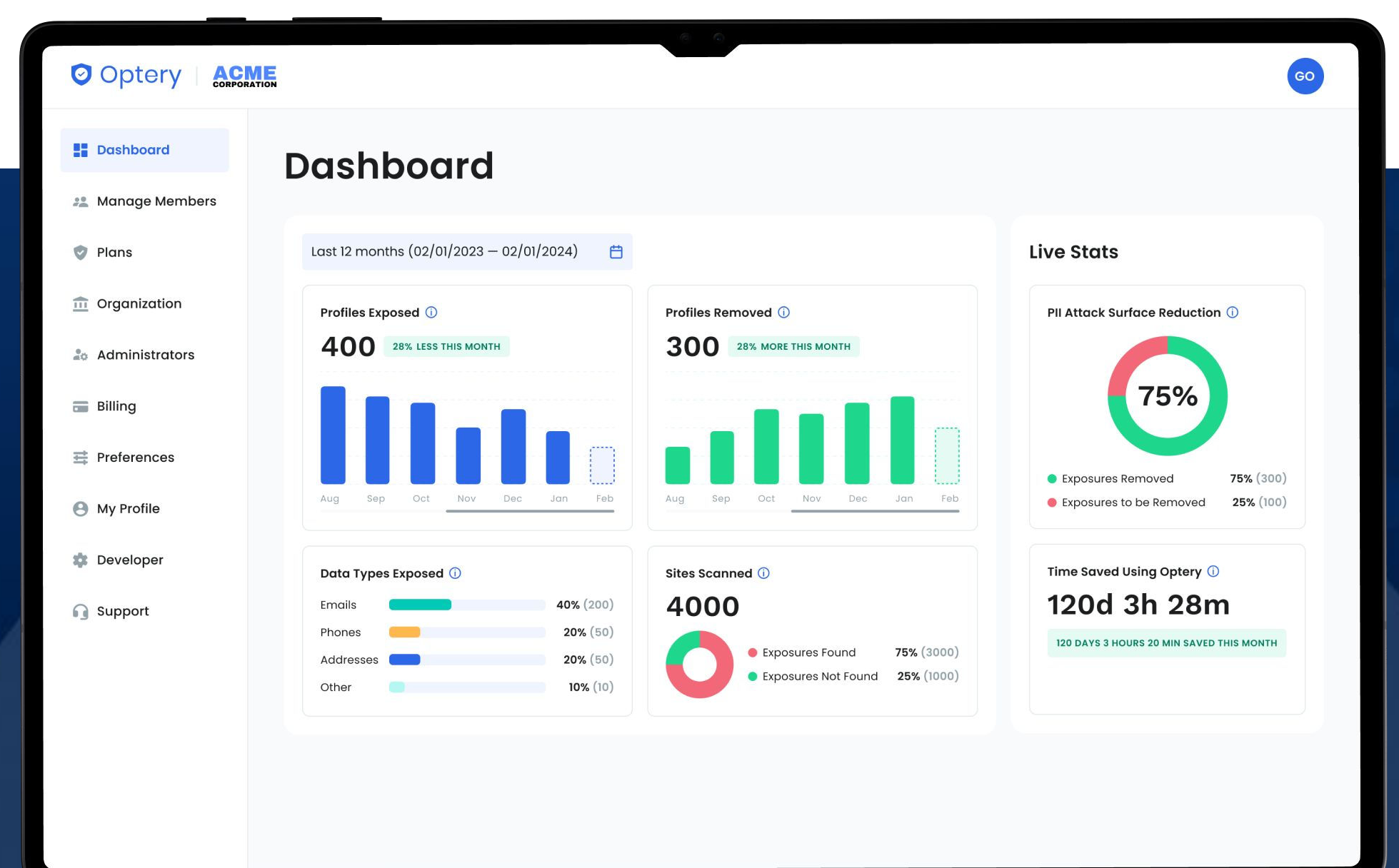
Detect new or republished data and execute automated removals with human validation.

Framework-Aligned Reporting

Help demonstrate measurable exposure reduction in support of financial-sector cybersecurity and risk management objectives.

What This Enables

- 1 Measurable reduction of externally exposed employee PII
- 2 Reduced phishing, smishing, and vishing attempts
- 3 Lower likelihood of credential compromise
- 4 Decreased digital and physical threat exposure



Powered by Optery Exposure Intelligence

Continuous discovery, high-precision removal, and measurable attack surface reduction.

PII ATTACK SURFACE

People-Search Sites & Business Info Aggregators

EXPLOITABLE DATA:

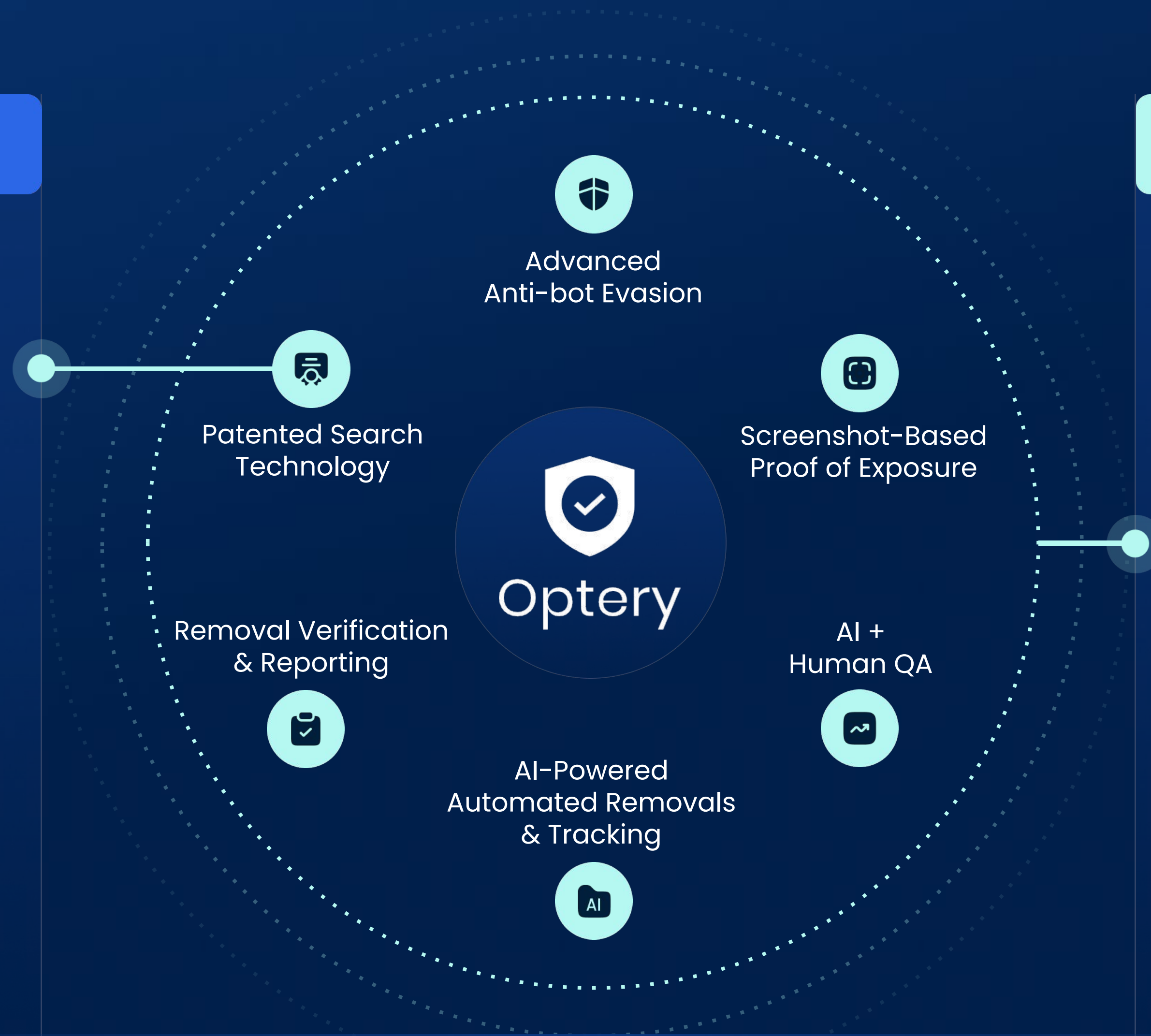
Personal & work phone numbers

Personal & work email addresses

Home address

Org-chart relationships

Household & relatives' linkage



BUSINESS OUTCOMES

Significantly reduced:

Social engineering risk

Account takeover (ATO) risk

Executive & employee physical threat exposure

Incident & alert volume

Continuous monitoring & removals

Optery identifies and eliminates the employee-specific data that fuels phishing, smishing, vishing, impersonation, credential theft, and real-world threats.



Book your demo at:

optery.com/get-your-optery-demo

 **FOR BUSINESS**

Protect Your Organization Against Social Engineering

Optery for Business empowers organizations to take a preemptive stance, uncovering and mitigating PII-based risks before they can be weaponized in AI-enabled social engineering attacks.

