DeleteMe

EBOOK

Deleting the Attacker's Advantage

How Human Attack Surface Management closes the gap between what attackers can find and what you can control.

01

In the Age of AI, Technology Risk Is No Longer Your Greatest Exposure

For decades, cybersecurity programs have invested resources in measuring and reducing technical exposure. They inventory internet-facing assets, identify vulnerabilities, map attack paths, and continuously monitor for misconfigurations. Far less attention has been paid to the publicly accessible information attackers can use to identify targets, build trust, and carry out social engineering attacks. The assumption was straightforward: if attackers wanted access to an organization, they would attack its technology.

That assumption is now dangerously incomplete.

60%

of breaches involved a human element in 2025

Source: Verizon, 2025 Data Breach Investigations Report

4.7x

more effective: phishing campaigns that leverage personal information vs. generic attacks

Source: Microsoft

A home address won't compromise a network. Neither will a phone number, a LinkedIn profile, or a list of former employers. But combined, these details create something far more valuable: a believable identity. And in modern social engineering attacks, believability is the difference between failure and access.

The more information attackers possess about a target, the easier it becomes to create believable pretexts, impersonate trusted individuals, and bypass the skepticism that security awareness training is designed to create. Attackers weaponize whatever's exposed. That used to mean infrastructure: servers, endpoints, cloud misconfigurations. Now it means your workforce. And weaponizing that exposure has never been easier.

This is the new layer of your attack surface. It's your people. We make it harder.

02

What Is Human Attack Surface Management?

Human Attack Surface Management (HASM)

The continuous discovery, assessment, and reduction of publicly available information attackers use to identify, impersonate, and socially engineer an organization's workforce.

For years, organizations treated publicly available information as a privacy concern. Today, it's a security concern. The same data that powers advertising, recruiting, and consumer profiling can also be used to identify targets, impersonate employees, and gain access to corporate systems. AI has accelerated this shift dramatically.

Five years ago, researching an employee required time, effort, and specialized OSINT skills. That's why attackers reserved highly personalized attacks for executives and other high-value targets. **Not anymore. It's not just the C-suite anymore. Anyone with access is a target.**

What used to take an attacker hours of manual research, AI can now do in seconds. Today, AI can build a dossier on every employee, generate convincing pretexts, and launch personalized phishing campaigns at scale, in any language, with no copywriting skill required. The economics of human reconnaissance have fundamentally changed, and they've changed in the attacker's favor.

89%

increase in AI-enabled attacks year over year

Source: CrowdStrike, 2025 Global Threat Report

82%

of detected initial-access attacks in 2025 involved no malware at all, only social engineering, credential theft, and identity-based techniques

Source: CrowdStrike, 2025 Global Threat Report

Most security controls are built to detect, block, or respond to attacks. HASM focuses on the phase of the attack lifecycle where social engineering is actually won or lost: **reconnaissance.** It's impossible to reduce exposure you can't see. The first step in any HASM program is understanding the human exposure your organization generates across data brokers, people-search sites, public records, social platforms, and other publicly accessible sources.

The harder it is for attackers to build a reliable profile of an employee, the more likely they are to make mistakes, get caught, or move on to an easier target. HASM isn't about detecting attacks. It's about making them uneconomical to execute in the first place. **That's the gap DeleteMe was built to close.**

03

How HASM Differs From Adjacent Categories

HASM is often confused with categories it overlaps with but doesn't duplicate.

CATEGORY	WHAT IT COVERS	WHAT IT MISSES
Attack Surface Management (ASM) / CTEM	Technical assets: internet-facing infrastructure, vulnerabilities, misconfigurations	Doesn't account for exposed personal or relationship data attackers use for social engineering
Digital Risk Protection (DRP)	Brand monitoring, executive impersonation, dark web mentions	Typically limited to executives or brand, not continuous coverage of the full workforce
Security Awareness Training / Human Risk Management	Training employees to recognize and resist phishing and manipulation attempts	Addresses behavior after exposure exists; doesn't reduce the underlying information attackers exploit
Personal Data Removal	Removing individual records from data broker and people-search sites	Often executed as a one-time, individual-level action rather than an ongoing, workforce-wide security program
Human Attack Surface Management (HASM)	Continuous discovery, assessment, and reduction of the public information attackers use to profile, target, and impersonate an entire workforce	Complements, rather than replaces, the categories above

HASM sits alongside CTEM as its human-layer counterpart. Where CTEM continuously validates exposure across technical assets, HASM continuously validates exposure across people. Both operate on the same principle: **you can't reduce what you haven't discovered, and you can't manage what you only check once.**

HASM is also distinct from human risk management and awareness training. Training changes how an employee *responds* to an attack. HASM changes how much *material* an attacker has to build that attack in the first place. The two work together, but one is not a substitute for the other, and organizations that only train while leaving exposure unmanaged are addressing the symptom rather than the source.

04

A Maturity Model for Human Attack Surface Management

Most organizations fall into one of four stages. Where does yours sit?

1

Unknown Exposure

No visibility into what's publicly discoverable about employees. Exposure has never been measured.

2

Reactive Removal

Ad hoc, one-time sweeps, usually limited to executives or triggered by a specific incident. No ongoing process.

3

Continuous Monitoring

Ongoing discovery and removal across data brokers, people-search sites, social platforms, and public records, extended across the workforce rather than just leadership.

4

Integrated HASM

Exposure data actively informs security awareness training, phishing simulation targeting, executive protection, and incident response, closing the loop between what's exposed and how the security program responds to it.

Most organizations we work with start at Stage 1 or 2. The goal of a HASM program is to move toward Stage 4, where exposure reduction isn't a one-time project but a continuously monitored input into the broader security program.

05

What Makes Up the Human Attack Surface?

A human attack surface consists of the exposed information attackers can use to learn about, profile, target, or impersonate people connected to an organization. It breaks down into two categories:

Personal Exposure	Professional Exposure
Home addresses	Job titles and responsibilities
Phone numbers	Reporting structures
Family relationships	Work histories
Property records	Conference appearances
Social media activity	Public professional profiles

But the human attack surface is bigger than individual employee data. Attackers don't just research individuals. They research **relationships.** They want to know:

- → Who reports to whom
- → Who has access to sensitive systems
- → Who approves payments
- → Who regularly interacts with executives

Every piece of information helps attackers build a more complete map of how trust flows through an organization. The more accurately they can reconstruct that map, the easier it becomes to identify targets, build believable pretexts, and manipulate normal business processes.

06

How Attackers Use the Human Attack Surface

The path from public information to compromised network typically follows four stages:

1 Reconnaissance

Attackers collect information from social media, corporate websites, public records, data brokers, and breached credential databases, assembling context on how people work, who they trust, and where they sit in the org.

2 Dossier-building

A job title reveals responsibilities. A LinkedIn profile reveals career history. An org chart reveals reporting lines. Together, these create a blueprint of how the organization operates and who's most likely to provide a path to access.

3 Targeting and pretexting

An HR employee receives a benefits-related request. A finance employee receives an invoice. A help desk technician receives a password reset request. The attack is tailored because the attacker already understands the role the target plays.

4 Escalation

Once attackers establish trust and gain a foothold, they rarely stop there. The phishing email or impersonation attempt is just the way in. From there, they escalate privileges, move laterally, and locate the systems that matter most.

Groups like **Scattered Spider** and **ShinyHunters** have used exactly this playbook: social engineering for initial access, followed by system lockdown and ransom demands, in some of the most disruptive breaches of recent years.

07

What Are the Benefits of Human Attack Surface Management?

Most security investments make attacks harder to *execute*. HASM makes attacks harder to *prepare*. The less information attackers can gather about employees, the harder it becomes to build a believable impersonation. That impact is measurable:

40%

reduction in phishing volume reported by DeleteMe customers

70%

reduction in sophisticated spear phishing attacks leveraging personal information

When security teams prioritize the human attack surface, attackers have less to work with. They spend more time researching targets, make more mistakes, and achieve lower success rates. Some give up and move on to easier targets entirely.

08

Retake Control of Your Human Attack Surface

Organizations spent the last decade reducing the attack surface of machines. The next step is about reducing the attack surface of people.

As AI continues to drive down the cost of reconnaissance, attackers no longer need to reserve personalized attacks for executives. They can run them at scale, across an entire workforce. **Deleting the Attacker's Advantage** means closing the gap between what attackers can find and what your organization can control, making your people harder to find, harder to fake, and harder to target. **DeleteMe makes this easy.**

QUICK SELF-ASSESSMENT

Is Your Human Attack Surface Exposed?

- [ ] Do you know how many employees currently have exposed home addresses, phone numbers, or family details across public data broker sites?
- [ ] Have you seen a recent increase in targeted phishing to employees outside your C-Suite?
- [ ] Could an attacker reconstruct your reporting structure using only LinkedIn and your company website?
- [ ] Do you have a continuous process for monitoring and removing employee exposure, or is it a one-time effort, if it's happened at all?
- [ ] Has your organization measured the impact personal data exposure has on your phishing and social engineering risk?

If you answered "no" or "not sure" to any of these, your human attack surface is likely larger than you think.

NEXT STEP

Ready to see what attackers can already see?

See exactly what's exposed across your workforce, and get a clear plan to close the gap.

Schedule a Human Attack Surface Assessment →

DeleteMe

About DeleteMe

DeleteMe is the leader in proactive privacy protection for organizations. We continuously find and remove employees' personal data from data brokers, people-search sites, and search results, shrinking the human attack surface that fuels phishing, impersonation, and AI-powered attacks. Our 100% US-hosted SaaS platform is SOC 2 and ISO 27001 certified.

250M+	1M+	150+
PII Removals	People Protected	Privacy Advisors