SpyCloud

2026 SPYCLOUD

IDENTITY EXPOSURE REPORT

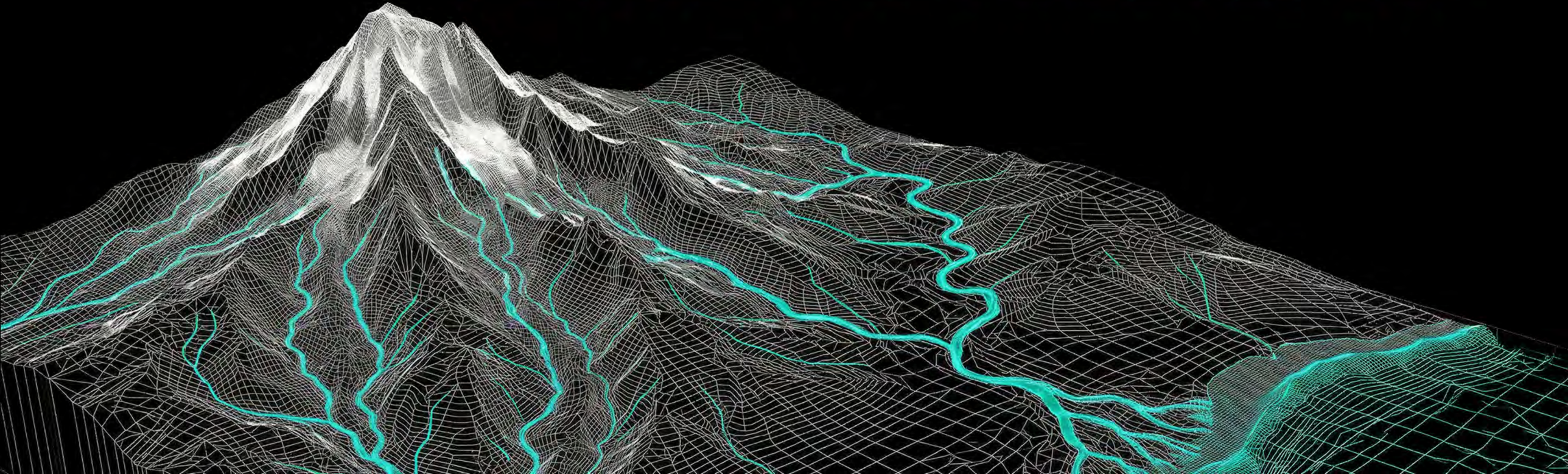
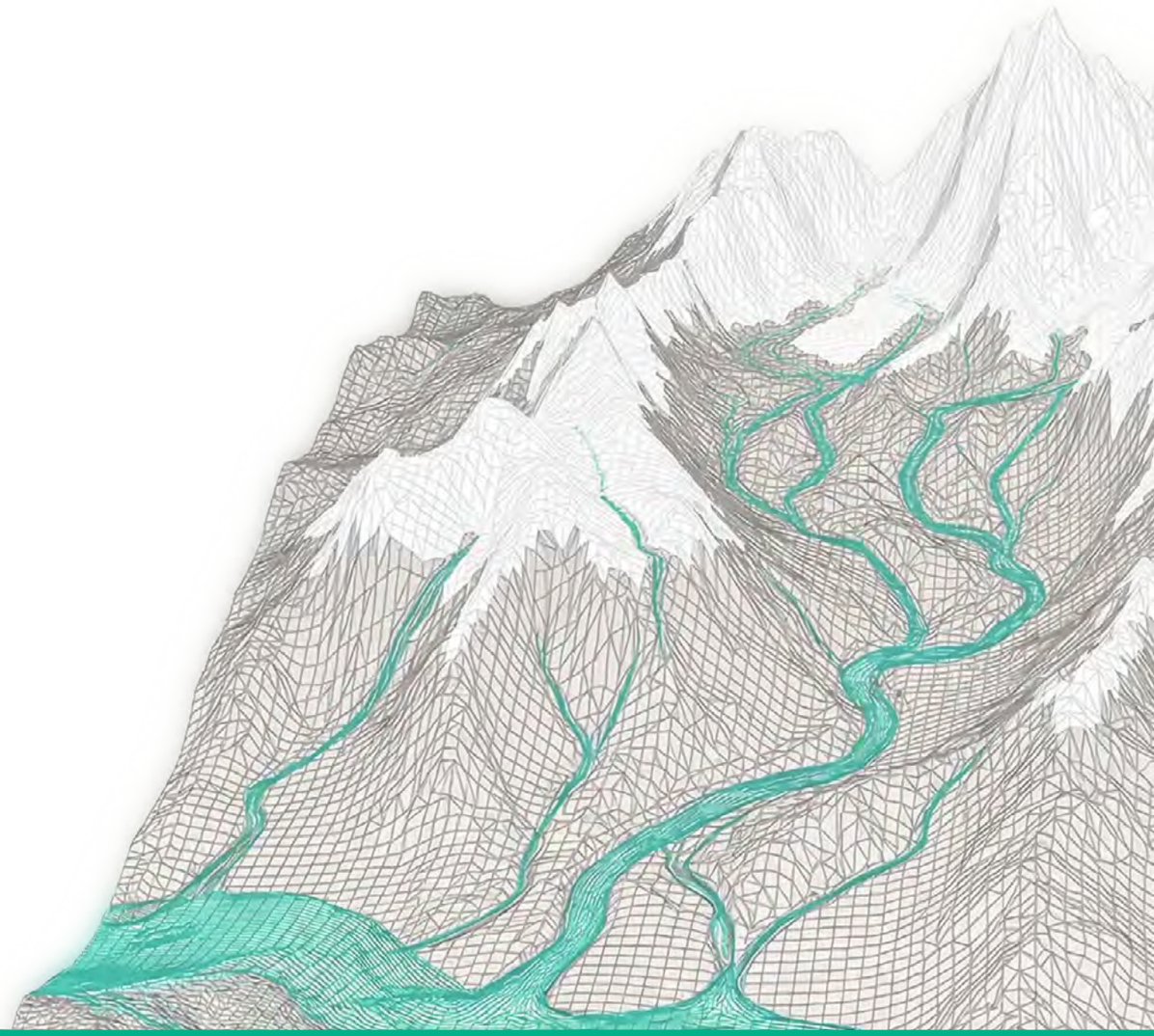
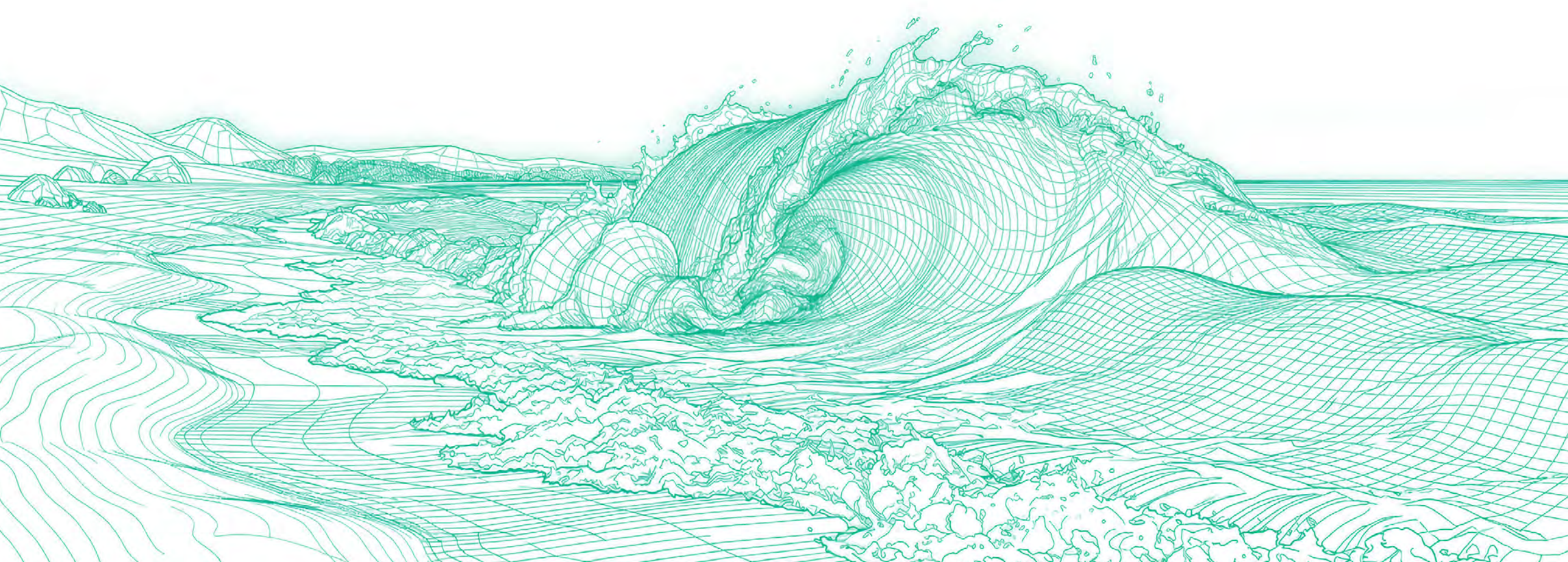


TABLE OF CONTENTS



CYBERCRIMINALS NOW HAVE MORE THAN 65 BILLION OPPORTUNITIES TO ATTACK

This report details SpyCloud's analysis of the now-flooded identity threat landscape – and what it means for the defenders tasked with protecting the human and non-human identity perimeter.



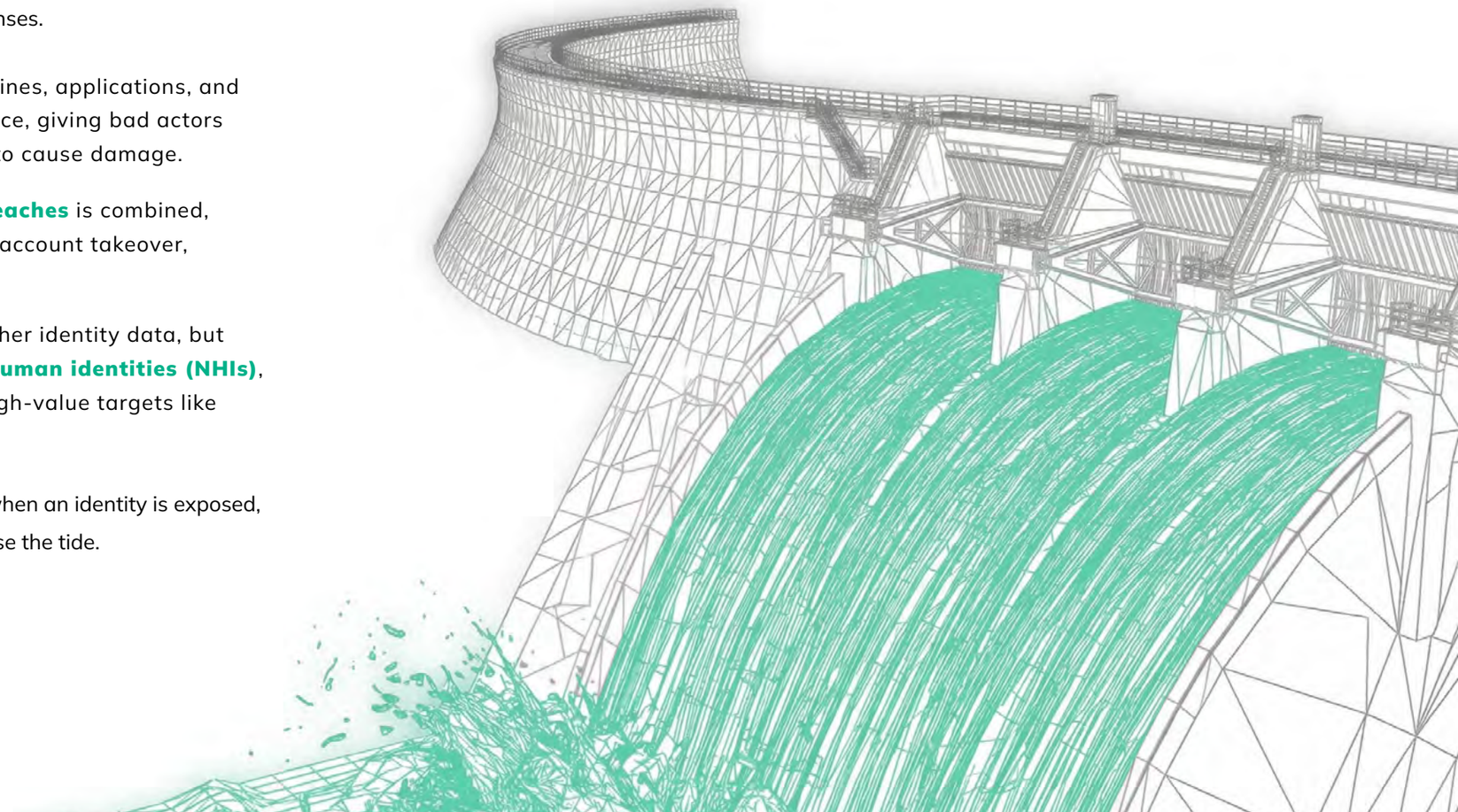
Over the last year, identity threats overran the berm. Spilled over and across the perimeter. Surging, seeping.

Here at SpyCloud, our datalake rose in response, expanding to **65.7B+ billion total distinct identity records** recaptured from the criminal underground – **a 23% increase from the previous year.**

This surge in exposed identity data reflects a fundamental shift in the volume of identity-based threats. Attackers have literally billions of options at their disposal to overwhelm defenses.

- Human and non-human digital footprints now sprawl across machines, applications, and systems. Each exposed identity fragment expands the attack surface, giving bad actors **more data, more initial access paths, and more opportunities** to cause damage.
- Stolen identity data from **phishing, infostealer malware, and breaches** is combined, packaged, and weaponized by attackers for follow-on attacks like account takeover, ransomware, session hijacking, and fraud.
- Attackers continue to steal credentials, session cookies, PII, and other identity data, but increasingly bypass user attributes altogether by **targeting non-human identities (NHIs)**, such as API keys, tokens, and service accounts, as well as other high-value targets like password managers and AI tools.

This year's report examines how identity sprawl perpetuates, what's at risk when an identity is exposed, and the practical steps security teams can take to reduce exposure and reverse the tide.



Important for understanding the data in this report

Through this report, we frequently refer to 'records' and 'assets' when speaking about identity exposure. Here's what we mean: An asset is a single data point associated with a digital identity. For example, an email address or password. A record is a collection of data points associated with a given digital identity, exposed via a single breach, malware infection, combolist, or phishing campaign. For example, a record could include an email address, password, IP address, and device details for a user.

INUNDATED BY EXPOSURES: THE 2026 IDENTITY EXPOSURE SURFACE*

TOTAL IDENTITY EXPOSURE

65.7B+ distinct identity records recaptured from the dark web

Last year, identity exposure was driven by:

INFOSTEALER MALWARE

13.2M
new infections

exposing **642.4M** credentials

averaging **50** exposed credentials per infection

PHISHING

28.6M
identity records

51%
of phished identities are consumers

49%
of phished identities are corporate users

DATA BREACHES

4,514
breaches, averaging 457K identity records per breach

There is still a deluge of exposed credentials circulating the dark web...

5.3B
credential pairs
(a 65% increase year-over-year)

38.5M
third-party application credentials
(a 450% increase year-over-year)

1.1M
master passwords for password managers

...as well as a new wave of exposed session cookies, AI tools, and NHIs

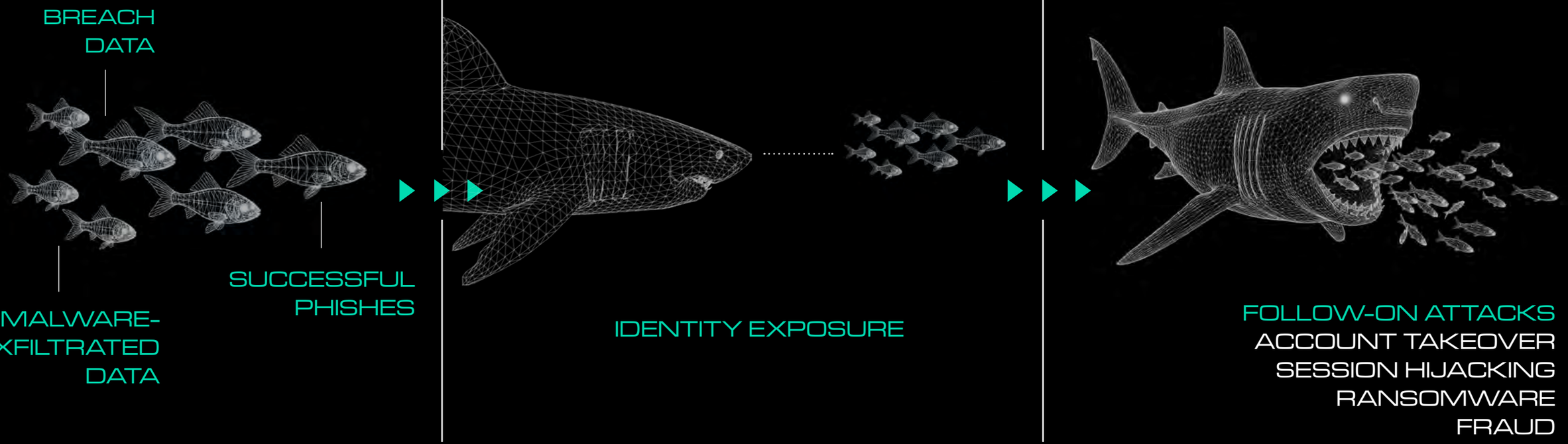
8.6B
stolen cookies

18.1M
API keys and tokens

6.2M
AI tool credentials and auth cookies

...GIVING BAD ACTORS MOMENTUM FOR TARGETED ATTACKS ON ENTERPRISE SYSTEMS, CLOUD PLATFORMS, AND ECOSYSTEMS.

*Figures reflect SpyCloud recaptured data from criminal underground sources.



EXPLOITING THE OVERFLOW: HOW ATTACKERS WEAPONIZE IDENTITY SPRAWL

Rapidly expanding human and non-human digital footprints are driving identity sprawl. Identity abuse becomes a fast follow.

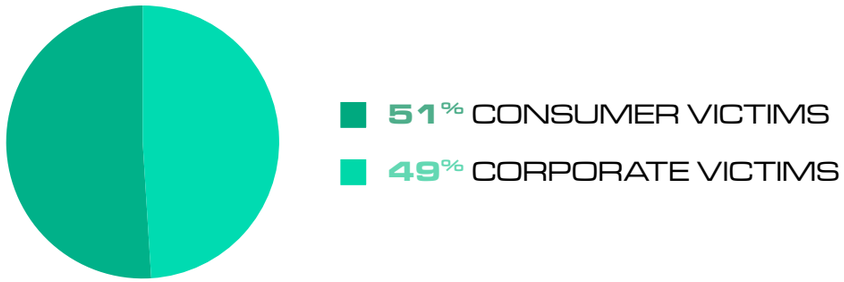
Phishing, malware, third-party breaches, and combolists feed vast volumes of identity data into the industrialized criminal ecosystem. The risk extends beyond compromise – it fuels costly attacks at scale. With so much exposed data in circulation, attackers can continuously piece assets together and use them to gain initial access across applications and systems to power follow-on attacks.

PHISHING: CASTING THE ENTERPRISE NET

Phishing remains the ***top-cited risk*** by security teams – and it's also the most-abused entry point for ransomware attacks. The most recent data supports the evidence that phishing is being used to target enterprises – probably with a higher success rate than you'd think. It's handing cybercriminals the keys to the kingdom, for enterprises and consumers alike.

PHISHING BY THE NUMBERS

» **28.6M** PHISHED IDENTITY RECORDS RECAPTURED IN 2025



Nearly half of all phished identities are corporate, and some kits have an even higher proportion of corporate victims, underscoring that enterprise controls are not stopping this threat.

EXAMPLE IN THE WILD

The Tycoon 2FA phishing-as-a-service (PhaaS) platform – which operates using an adversary-in-the-middle (AitM) approach – captures sensitive authentication tokens from its victims that can be replayed later to gain unauthorized access without re-entering MFA. SpyCloud contributed to disruption efforts targeting Tycoon 2FA in 2026 and performed a ***victimology analysis*** that showed that approximately **80%** of victims were in fact enterprise users.

This high-volume identity exposure tactic captures more than usernames and passwords.

» **50%** OF PHISHED RECORDS CONTAINED AN EMAIL ADDRESS

» **49%** CONTAINED LOCATION DATA LIKE IP OR PHYSICAL ADDRESS

WHAT MODERN PHISHING CAPTURES

Today's phished datasets increasingly contain high-fidelity identity data, not just credentials:

- SESSION COOKIES
- AUTHENTICATION TOKENS
- 2FA SECRETS
  - ONE-TIME PASSCODES
  - MFA APPROVAL WORKFLOWS

Modern phish kits set up a proxy for victims to authenticate against the real application, complete 2FA, and then allow a bad actor to take over the active session and impersonate the victim.

HOW PHISHING FEEDS IDENTITY SPRAWL

Cybercriminals have industrialized phishing, using AI-driven phishing campaigns and phishing-as-a-service (PhaaS) platforms to make data theft easier and more convincing than ever.

ABOUT PHAAS PLATFORMS

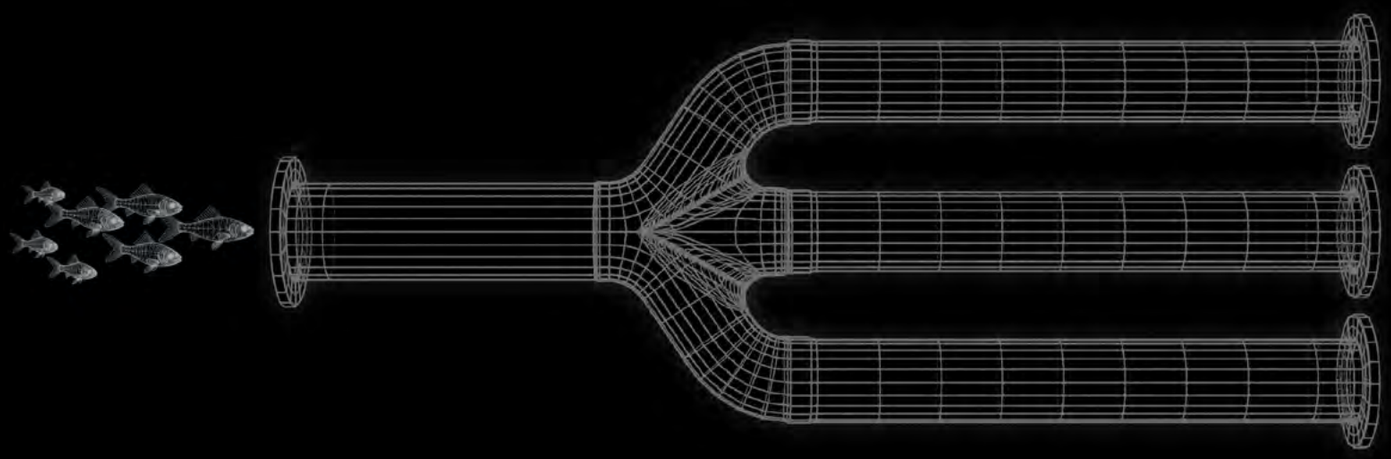
PhaaS platforms like Tycoon 2FA package sophisticated attack capabilities into ready-made, subscription-based toolkits that require little to no technical skill to deploy. By commercializing the phishing process – complete with fake website designs, MFA-bypass capabilities, and even victim-vetting mechanisms with pre-built email templates – these platforms have democratized access to advanced attack tactics, flooding the threat landscape with a wave of new, low-skilled actors capable of executing enterprise-grade attacks.

THE IMPACT IS MEASURABLE

SpyCloud research shows **94%** of Fortune 50 companies have employee data exposed in phishing attacks.

WHAT ATTACKERS DO WITH PHISHED IDENTITY DATA

Layered on top of AI-driven personalization and infostealer malware that feeds criminals richer targeting data, PhaaS has made phishing the dominant initial access vector for ransomware and account takeover. It's the starting point for more damage:



Abuse credentials or session data
to gain initial access to systems

Launch account takeover
to lock out users and commit fraud

Carry out lateral movementa
to compromise assets in support of ransomware or other attacks

MALWARE BE DAMMED, BUT NOT DETERRED

Global law enforcement operations disrupted several high-profile infostealers in the past year, reducing activity from dominant families and forcing the ecosystem to adapt. While these efforts – supported by intelligence and expert resources from organizations like SpyCloud – have had measurable impact, infostealers remain one of the most reliable sources of high-fidelity identity data for attackers, continuing to expose credentials, cookies, and other sensitive data around the clock.

FALSE SENSE OF SECURITY

40% of malware infections occurred on endpoints with EDR or antivirus tools installed last year, demonstrating that attackers routinely bypass traditional endpoint defenses to steal identity data

PARTNERS IN DISRUPTING CRIME

SpyCloud partners with private, public, and non-profit organizations as well as community researchers and volunteers that share a commitment to ***disrupting cybercrime operations*** and protecting the digital economy to enable faster takedowns, target remediation, and create a safer internet for all.

OSINT FOUNDATION℠ · Operation Endgame · Cybercrime Atlas · AFCEA · Potomac Officers Club

INFOSTEALER MALWARE BY THE NUMBERS

13.2M INFOSTEALER LOGS
RECAPTURED FROM INFECTIONS IN 2025

DOWN FROM **18M** THE PREVIOUS YEAR FOLLOWING COORDINATED LAW-ENFORCEMENT ACTION, SUPPORTED BY SPYCLOUD'S IDENTITY INTELLIGENCE

642.4M CREDENTIALS AND 8.6B COOKIES
EXFILTRATED BY MALWARE INFECTIONS

INCLUDING **38.5M** THIRD-PARTY APPLICATION CREDENTIALS EXPOSED

MORE THAN **5X** INCREASE
YEAR OVER YEAR

Malware-exposed credentials, session cookies, and other identity data are used to:

- **Hijack valid sessions** using stolen cookies or tokens
- **Take over accounts** across corporate and SaaS environments
- **Move laterally** and launch data theft extortion or ransomware attacks
- **Resell access** in underground markets for follow-on abuse

BREACHES & MEGABREACHES: DROWNING IN OLD DATA

Data breaches expose credentials and identity data, often at massive scale.

DATA BREACH EXPOSURE BY THE NUMBERS

This high-volume identity exposure tactic captures more than usernames and passwords.

» **4,514** DATA BREACHES RECAPTURED IN 2025

▲ **27%** from 3,562 the prior year

» **39** OF THOSE BREACHES CONTAINED **50M+** RECORDS

» **456,000** RECORDS EXPOSED PER BREACH, ON AVERAGE

WHAT MODERN WHAT ATTACKERS DO WITH EXPOSED ENTERPRISE DATA

Credentials exposed in data breaches are reused to:

» **BYPASS** ALERTS AND CONTROLS BECAUSE ACCESS APPEARS LEGITIMATE

» **GAIN ACCESS TO ENTERPRISE SYSTEMS** INCLUDING CLOUD PLATFORMS AND BUSINESS-CRITICAL APPLICATIONS, TO LAUNCH FOLLOW-ON ATTACKS

» **TAKE OVER CONSUMER ACCOUNTS** TO COMMIT FRAUD

» **FEED OPPORTUNITIES FOR OTHER TACTICS** LIKE MALWARE INFECTIONS AND PHISHING TO STEAL OR EXFILTRATE ADDITIONAL DATA

WHY "MEGABREACH" HEADLINES CAN BE MISLEADING

While many can, not all data breaches represent net-new identity risk. Many large-scale breach disclosures rely on ***recycled URL:Login:Password (ULP) combolists***, not newly stolen data.

In a sample of SpyCloud combolist data, **51%** of records overlapped with existing infostealer logs, indicating reuse rather than fresh compromise. Some high-profile sources (***example, the ALIEN TXTBASE combolist***) showed **60-80%** overlap with previously observed stealer data, along with incomplete records and signs of fabricated credentials. This overlap highlights the recent shift in combolists repackaging credentials from malware infostealers, making them even more valuable to other criminals than historic combolists based on third-party breach data.

Because combolists often aggregate recycled or lower-quality data, SpyCloud applies strict ingestion and deduplication controls, prioritizing datasets with demonstrable volumes of **new, non-duplicative credentials** to avoid duplicate signals and unnecessary alerts for defenders.

NON-HUMAN IDENTITIES: THE FASTEST-GROWING BRANCH OF THE ATTACK SURFACE

The emerging trends we observed in 2025 had a recurring theme: malicious actors are taking full advantage of the expanding digital identity, including the non-human component. We recaptured **18.1 million** NHIs last year alone, including:

Non-human identities (NHIs), including API keys, tokens, secrets, service accounts, and automation credentials, allow applications and systems to authenticate without a human present. Because these identities are persistent, often over-privileged, and rarely governed with the same rigor as human accounts, they have become a preferred target for attackers seeking persistent access with minimal risk of detection.

Unlike user credentials, NHIs are designed to operate continuously. When exposed, they allow attackers to bypass traditional identity controls such as MFA, automate abuse, and expand access across interconnected systems in an unfortunate ripple effect.

60K+
API keys and tokens tied to payment and remittance platforms

36K+
tokens for infrastructure and hosting platforms like AWS, Google, and Microsoft

3.3K+
developer platform tokens for platforms like Atlassian and GitHub

Hundreds
of API keys from widely available AI platforms including OpenAI and Anthropic

Dozens
of exposed tokens associated with software package repositories including PyPi and NPM

1.3K+
Slack API tokens

*Note: These platforms are not the source of the risk. They are actively targeted because they are deeply embedded across modern development, infrastructure, and collaboration workflows.

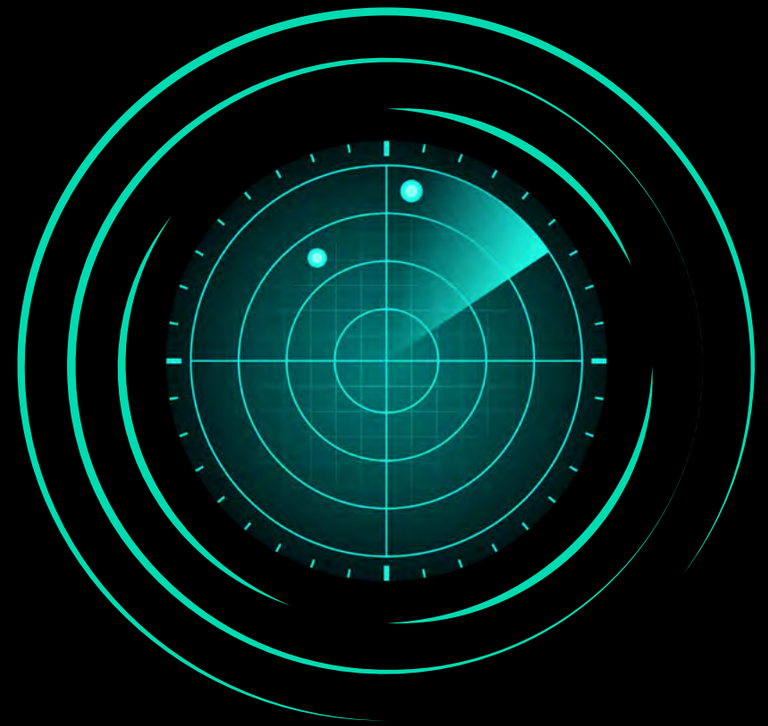
ATTACKERS ARE TARGETING HIGH-IMPACT NHIs

Attackers are increasingly prioritizing NHIs that sit deep inside trusted workflows and offer disproportionate downstream impact when exposed.

AI platform credentials illustrate this shift. While they appear in lower volume today, SpyCloud observed a **significant year-over-year** increase as organizations embed AI tools into proprietary data pipelines, models, and workflows.

6.2M CREDENTIALS OR AUTHENTICATION COOKIES FOR AI TOOLS RECAPTURED

The same pattern is evident in package repository tokens, one of the highest-risk NHI exposure types. When compromised, these credentials can be used to introduce malicious code into trusted software supply chains, enabling large-scale downstream compromise and propagating access far beyond the original exposure.



WHY ATTACKERS PREFER NON-HUMAN IDENTITIES

Attacks against payment, infrastructure, and software package platforms increasingly focus on token theft and reuse, rather than traditional credential phishing. NHIs offer attackers:

- LACK OF MFA OR STRONG IDENTITY ASSURANCE
- LIMITED ROTATION AND OFTEN UNCLEAR OWNERSHIP
- BROAD, LONG-LIVED PERMISSIONS
- DETECTION DEPENDENT ON ANOMALOUS USAGE – OFTEN AFTER DAMAGE IS DONE

As a result, compromised NHIs provide attackers with persistent, low-visibility access and a faster path to lateral movement across environments.

PASSWORDS – STILL A PREMIUM CATCH FOR CYBERCRIMINALS

Despite years of security awareness and defensive tooling, passwords remain the most common – and most damaging – element inside exposed identities. Reuse, plaintext storage, and infrequent resets continue to make passwords a reliable accelerator for automation, repeat compromise, and large-scale abuse.

PASSWORD EXPOSURE BY THE NUMBERS

SpyCloud's 2025 research reveals the vastness of the exposed credentials (email/username + password combo) circulating within the criminal underground:

- **5.3B** TOTAL RECAPTURED CREDENTIAL PAIRS
- **PASSWORD REUSE RATES**
  - **7** IN **10** CONSUMERS HAVE REUSED AN EXPOSED PASSWORD
  - **4** IN **10** CORPORATE USERS HAVE REUSED AN EXPOSED PASSWORD

PLAINTEXT PASSWORD EXPOSURE

Plaintext passwords continue to appear at scale, dramatically lowering the barrier to immediate account takeover and offering a pathway to credential stuffing attacks.

- **80%** OF EXPOSED CORPORATE CREDENTIALS INCLUDED A PLAINTEXT PASSWORD
- **63%** OF EXPOSED CONSUMER CREDENTIALS INCLUDED A PLAINTEXT PASSWORD

1.1M PASSWORD MANAGER MASTER PASSWORDS RECAPTURED IN 2025

TOOLS DESIGNED TO CENTRALIZE ACCESS AND INCREASE PRODUCTIVITY ARE INCREASINGLY PRESENT IN EXPOSURE DATA TOO, RAISING THE STAKES OF IDENTITY COMPROMISE.

While the transition to ***passwordless*** is happening all around us, traditional passwords and particularly master passwords remain weak spots to be exploited. The master password is user-generated, leading to the same risks with even greater consequences by exposing the entire vault.

TRENDY PASSWORDS: THE COST OF PREDICTABILITY

Human behavior continues to reinforce password reuse and abuse. Predictable patterns tied to pop culture, sports, and simple numeric strings appear consistently across exposure data.

Top trendy passwords:

67 / sixseven: **140.4M**
123456: **20.1M**
sweet / cookie / candy / cake / pie: **5.7M**
chiefs / kansas city chiefs: **5.0M**
2025: **4.1M**
password: **3.3M**
admin: **3.1M**
apple / banana / orange / strawberry / fruit: **2.6M**

PASSWORD EXPOSURE & BEYOND IN THE SUPPLY CHAIN

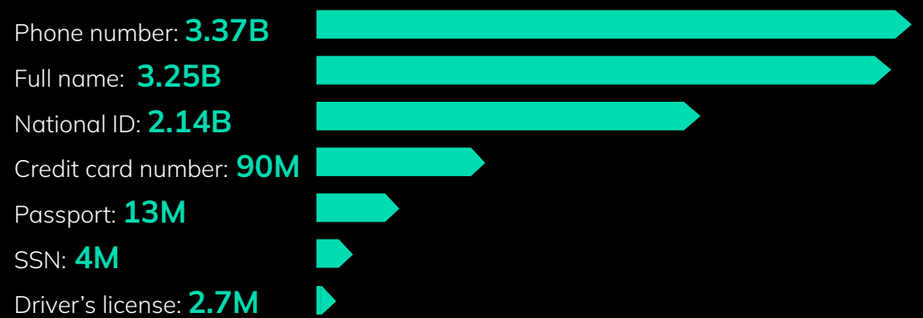
SpyCloud helps organizations identify **when third-party and vendor application credentials and other identity data are exposed** – not just when their own users or domains appear in data circulating the criminal underground. By mapping exposures back to specific applications and services, security teams can prioritize remediation, and cut off attacker pivot opportunities before they're exploited.

Learn about Supply Chain Threat Protection >>

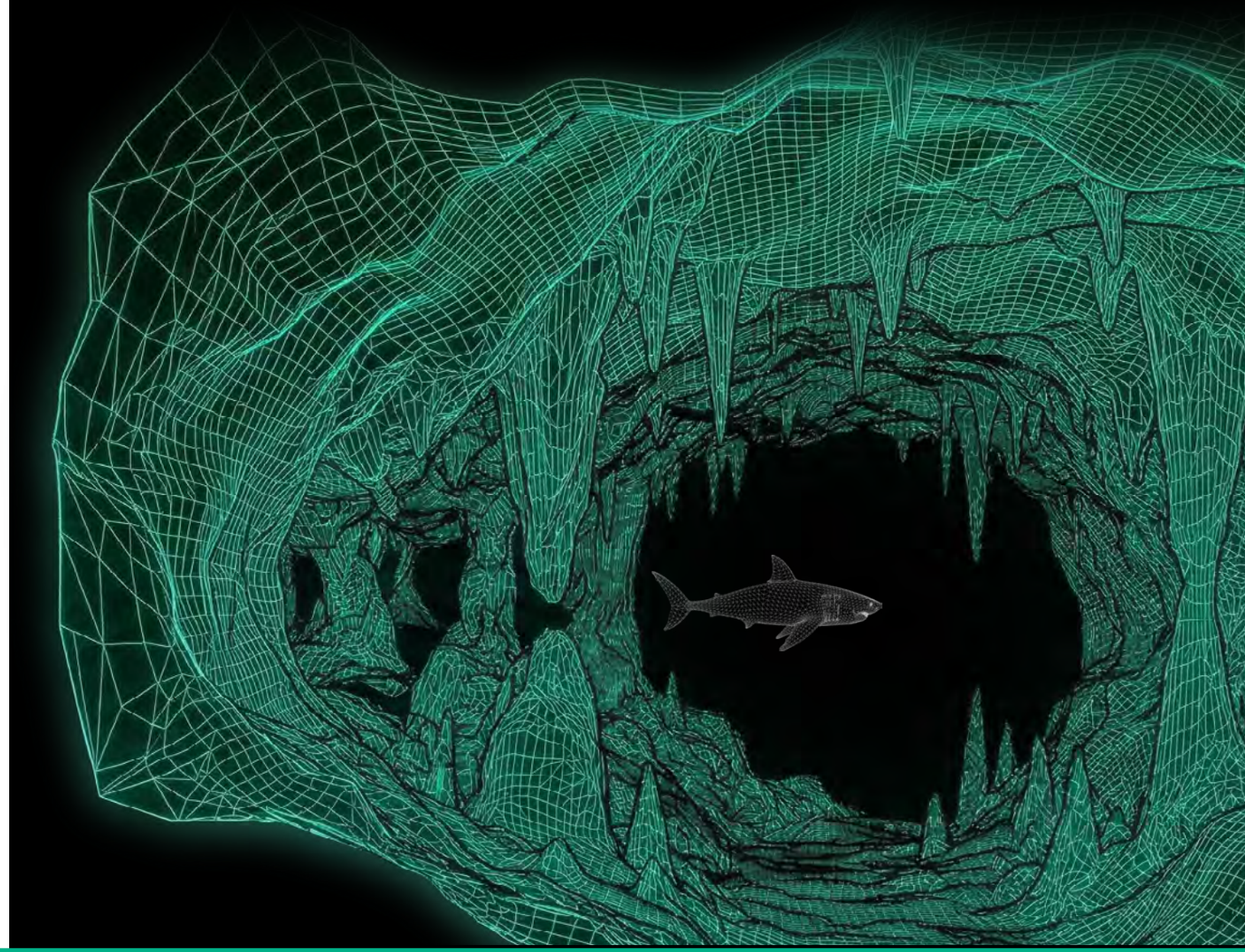
PII KEEPS FLOWIN'

Passwords are rarely exposed alone. They're often captured alongside a bounty of additional personally identifiable information (PII), giving attackers both authenticated access and the context needed to commit fraud and abuse.

PII EXPOSED LAST YEAR



ONCE IDENTITY DATA FLOWS INTO **THE CRIMINAL UNDERGROUND**, IT TAKES ON A LIFE OF ITS OWN, MORPHING AND SHAPING DOWNSTREAM IDENTITY-BASED THREATS.



THE IDENTITY ATTACK SURFACE RUNS WIDE & DEEP – YOUR DEFENSES SHOULD TOO

Human and non-human identity sprawl fundamentally changes how identity threats must be managed. As we witness continuous exposure occur at scale, it's imperative we implement continuous monitoring and remediation.

SPYCLOUD'S IDENTITY THREAT PROTECTION MATURITY MODEL

Rather than attempting to eliminate exposure entirely, high-performing security programs focus on progressive threat reduction, eliminating attacker opportunity even when exposure occurs.

WHAT THIS MEANS FOR DEFENDERS

Identity exposure is inevitable, but you can influence how much damage it causes. Organizations that treat identity sprawl as a measurable, manageable attack surface – rather than a series of isolated incidents – are best positioned to reduce compromise, contain damage, and disrupt attacker economics over time.

LEVEL 1 – DEFEND

Remove the most common paths to initial access

- » Reduce password reuse and enforce phishing-resistant MFA
- » Identify and rotate known-exposed credentials
- » Monitor for workforce and consumer identity exposures stemming from breaches, phishing, and malware infections

Goal: Eliminate easy wins for attackers.

LEVEL 2 – DEEPEN

Implement comprehensive exposure monitoring and containment capabilities

- » Remediate workforce and consumer identity exposures, both historical and new
- » Invalidate exposed sessions, cookies, and tokens to reduce session hijacking risk
- » Expand identity exposure visibility to vendor and other third-party identities
- » Inventory non-human identities, assign ownership, and document usage
- » Enforce rotation and least-privilege access for API keys, tokens, and service accounts

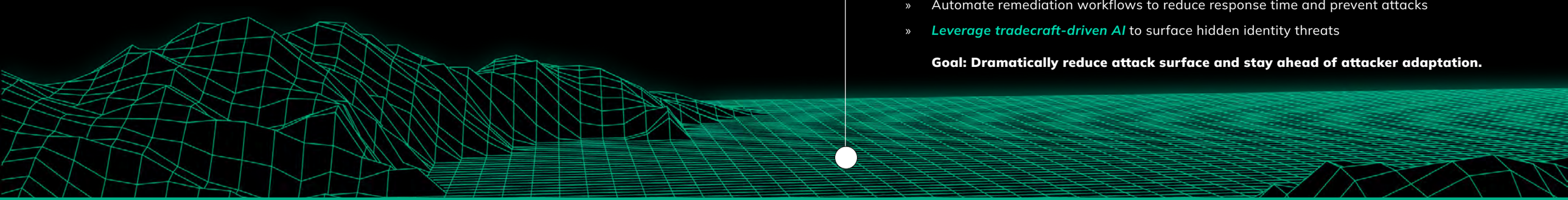
Goal: Reduce exposure radius across human and non-human access paths.

LEVEL 3 – DISRUPT

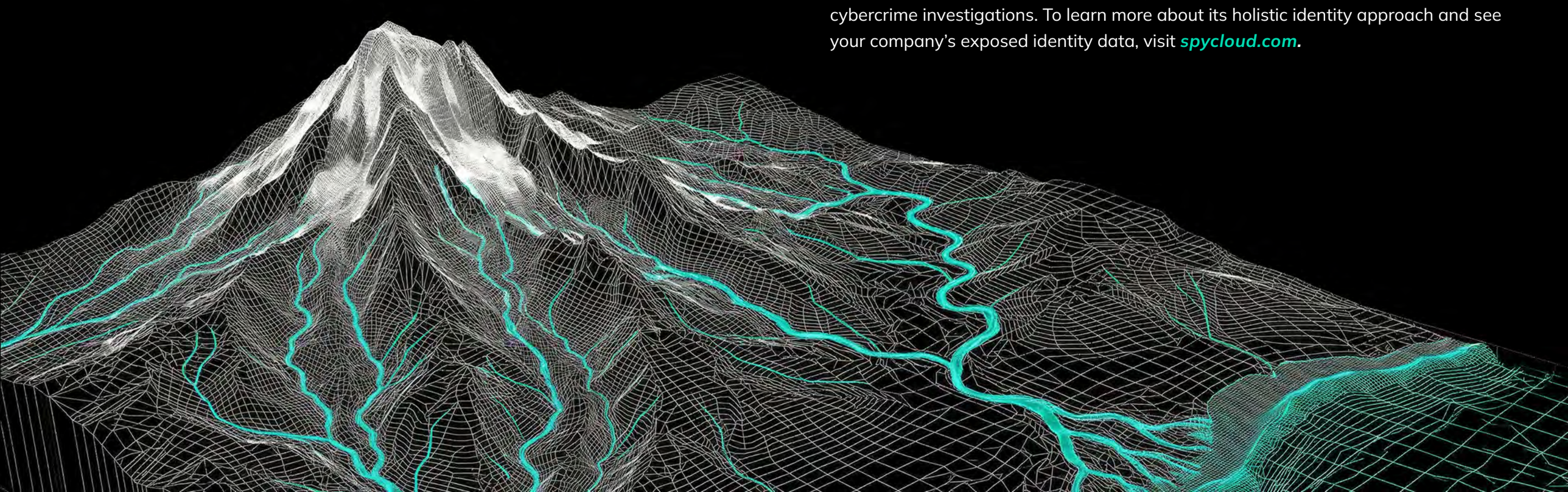
Proactively break attack cycles with advanced identity threat protection

- » Continuously monitor for exposed identities across human and machine accounts
- » Automate remediation workflows to reduce response time and prevent attacks
- » ***Leverage tradecraft-driven AI*** to surface hidden identity threats

Goal: Dramatically reduce attack surface and stay ahead of attacker adaptation.



SpyCloud



ABOUT SPYCLOUD

WE'RE 10 YEARS IN, AND WE WON'T STOP 'TIL BAD ACTORS DO.

SpyCloud protects businesses from the stolen identity data criminals are using to target them now. Its automated identity threat protection solutions leverage advanced analytics and AI to proactively prevent ransomware and account takeover, detect insider threats, safeguard employee and consumer identities, and accelerate cybercrime investigations. To learn more about its holistic identity approach and see your company's exposed identity data, visit ***spycloud.com.***