

INSIDE THE CRIMINAL UNDERGROUND: POST-AUTHENTICATION IDENTITY THREATS

ABOUT SPYCLOUD

SpyCloud is the world's leading Identity Threat Protection company, enabling organizations to **continuously detect and automatically remediate compromised identities** *before* attackers exploit them



OUR SOLUTIONS

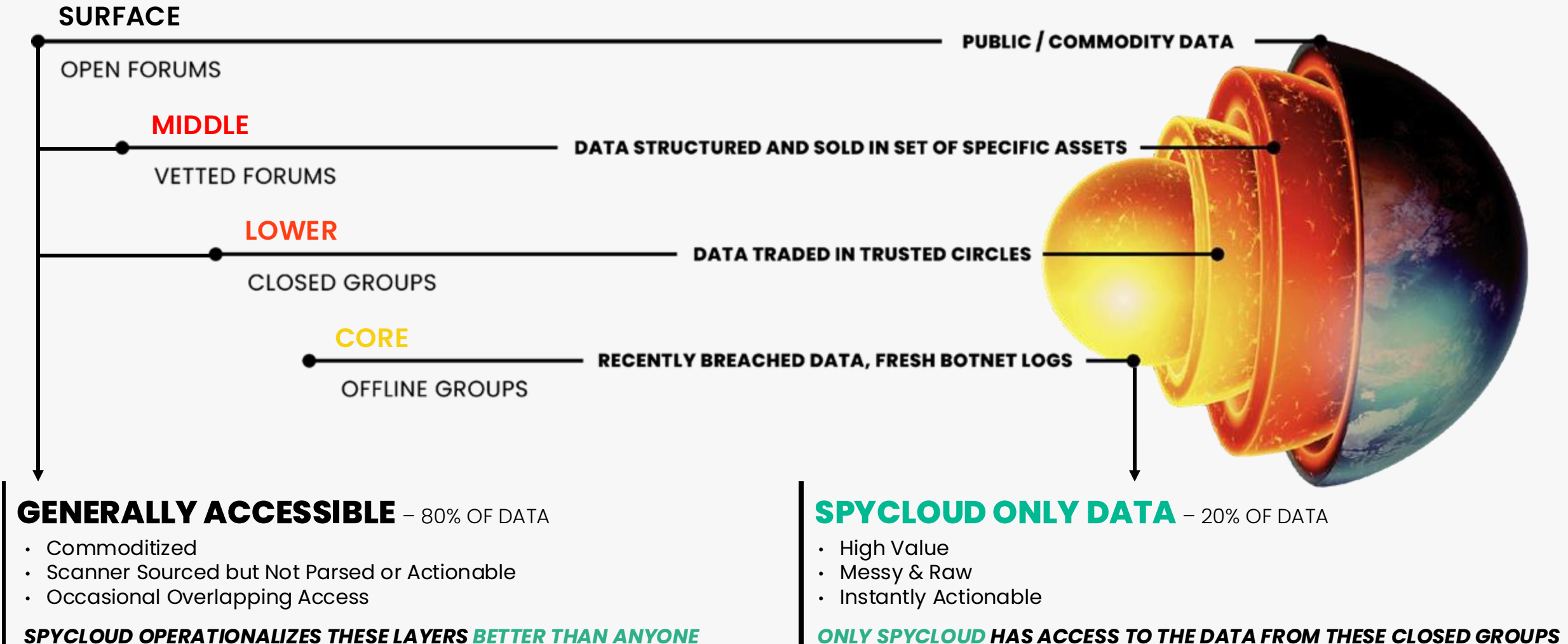
- Protect enterprises from cyberattacks & insider threats
- Safeguard consumer identities from fraud
- Power cybercrime investigations, with resolution in seconds

600+ CUSTOMERS • PROTECTING 4B+ ACCOUNTS • IT IDENTITY ASSETS • 300+ INTEGRATIONS

WHY SPYCLOUD

SpyCloud

The industry's largest originator of recaptured darknet data



How Exposed Are You?

OF THE 80+ COMPANIES ATTENDING THIS EVENT

MALWARE

19,147

EXPOSED MALWARE
RECORDS

RECAPTURED FROM MALWARE INFECTED EMPLOYEES

PHISHING

36,348

PHISHED EMPLOYEE
ASSETS

CREDENTIALS AND IDENTITY DATA HARVESTED IN
SUCCESSFUL PHISHES

COOKIES

2M+

STOLEN SESSION
COOKIES

VIA MALWARE AND PHISHING ACROSS EMPLOYEES

DATE RANGE: Based on the last 12 months of exposure data from September 1, 2025 to September 1, 2026

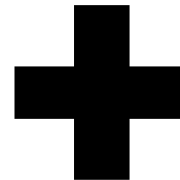
UNDERSTANDING THE *SURGING* IDENTITY ATTACK SURFACE

PHISHED VICTIMS

Phishing is now the **#1** entry point for ransomware – stealing far more than just passwords

NON-HUMAN IDENTITIES

SpyCloud recaptured 18 million+ exposed **API key and tokens**



ENDPOINT SECURITY GAPS

66% of recaptured malware data came from devices running endpoint protection

SUPPLY CHAIN THREATS

Third-party involvement in breaches jumped **60% YoY to 48%**

TOP-OF-MIND THREATS

GETTING PAST MFA

SpyCloud

These threats are visible in recaptured data **before an incident occurs** – demonstrating the power of identity threat **protection**.



Adversary-in-the-middle phishing (AiTM)

A proxy page relays the login in real time and captures the authenticated session – a critical gap in passwordless environments.

SPYCLOUD DELIVERS

Stolen access details from successful phishes + automated revocation of sessions and password resets via native and custom integrations.



Session hijacking

Stolen cookies let a criminal resume a valid session without credentials, bypassing MFA and event passkeys.

SPYCLOUD DELIVERS

Real-time infected user, device and application details – including cookies per application – and automated session invalidation for post-infection remediation.



Remote worker fraud

A fraudulent hire clears onboarding with a synthetic or stolen identity and gains insider access.

SPYCLOUD DELIVERS

AI-powered detection and investigation of correlated aliases and personas, so candidate identities can be checked against known criminal ties.

VOLUME, VARIETY & FRESHNESS OF DATA

VOLUME

**1 trillion
identity assets**

Exposures you likely haven't seen, from sources no other provider has – pointing to where criminals are headed next

VARIETY

**Malware, Phishes,
Breaches, Combolists,
Chatter**

5 sources continuously recaptured from criminal communities, all in 1 platform

FRESHNESS

**Continuous
delivery**

Data is ingested all day, every day – detecting identity compromise in real time for immediate response

KEY TAKEAWAYS

Tips for Securing your Workforce Identity

1 AUTHENTICATION ≠ LOGIN

Attacks use stolen identity artifacts to bypass MFA and security controls

2 PHISHING = ENTERPRISE THREAT

New phishing campaigns no longer rely on spoofed Login pages

3 MALWARE = ACTIVE THREAT

Indicates compromised device – requires immediate incident response and full remediation

4 COMBOLISTS MATTER

Repackaged ULP:Combolist contains identity data from infostealer logs

5 HOLISTIC IDENTITIES

Hidden exposures (past and present, work and personal) tied to workforce identities – expanding the attack footprint & entry points

IDENTITY THREAT PROTECTION SOLUTIONS

ENTERPRISE PROTECTION

SAFEGUARD EMPLOYEE IDENTITIES

- WORKFORCE THREAT PROTECTION
- ENDPOINT THREAT PROTECTION
- SUPPLY CHAIN THREAT PROTECTION
- SESSION IDENTITY PROTECTION

ACT ON KNOWN POINTS OF
COMPROMISE BEFORE THEY CAN BE
USED BY CYBERCRIMINALS

CONSUMER PROTECTION

PROTECT CONSUMER IDENTITIES

- CONSUMER THREAT PROTECTION
- SESSION IDENTITY PROTECTION
- FINANCIAL THREAT PROTECTION
- FRAUD PREVENTION
- DARK WEB MONITORING

STOP HIGH-RISK ATTACKS TIED TO
MALWARE AND PROACTIVELY
PREVENT FRAUD

INVESTIGATIONS

CONNECT IDENTITY ASSETS

- THREAT ACTOR ATTRIBUTION
- INSIDER THREAT DETECTION
- INFECTED HOST IDENTIFICATION
- VIP EXPOSURE VERIFICATION
- FINANCIAL CRIMES ANALYSIS

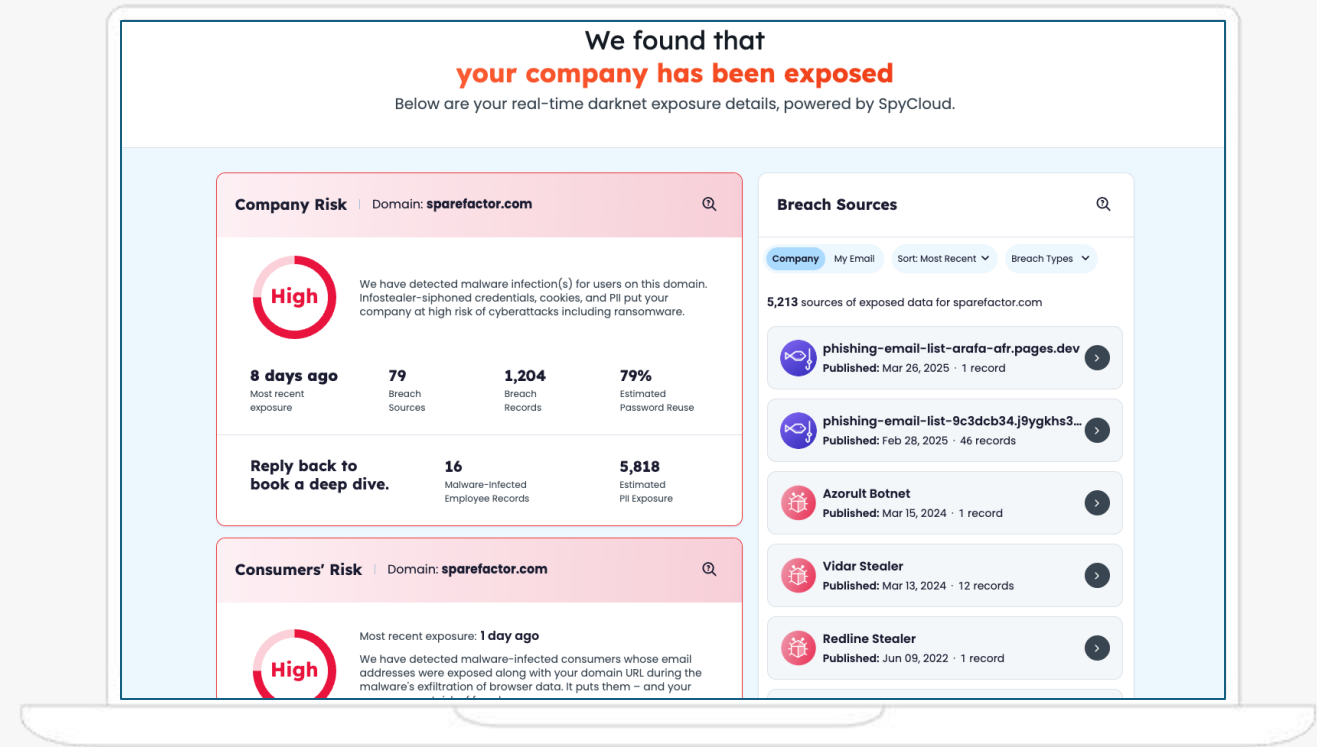
UNCOVER HIDDEN RELATIONSHIPS
AND CONNECTIONS ACROSS
IDENTITY ASSETS

CHECK YOUR DARKNET EXPOSURE

SEE WHAT CRIMINALS KNOW ABOUT YOUR BUSINESS

Identify threats from exposed identities, with details into real-time exposures including:

- Malware-infected employees
- Stolen session cookies
- Recency of breach exposures
- Exact sources, dates and more



spycloud.com

CHECK YOUR EXPOSURE