OWASP®
Los Angeles

SpyCloud

Presentation by J.R. Rulison
jr.rulison@spycloud.com

SpyCloud
IDENTITY
THREAT PROTECTION

SpyCloud

THE MISSION

We exist to disrupt cybercrime

As the leader in **identity threat protection**, our solutions thwart cyber attacks that originate from the use of stolen identity data, including account takeover, ransomware, and online fraud – and **protect more than 4 billion accounts worldwide.**

- **Protecting your enterprise from cyberattacks**
- **Safeguarding your consumer identities**
- **Powering cybercrime investigations**

Automated ATO Prevention | Ransomware Prevention | Continuous Zero Trust | Fraud Prevention | Session Hijacking Prevention | Threat Actor Attribution | Dark Web Monitoring | Insider Threat Detection | Supply Chain Threat Protection

USE CASES

CUSTOMERS INCLUDE

standard chartered · U.S. DEPARTMENT OF ENERGY · CVSHealth · ATLASSIAN · CHIPOTLE MEXICAN GRILL · lendingtree · Canva

WHY SPYCLOUD

SpyCloud

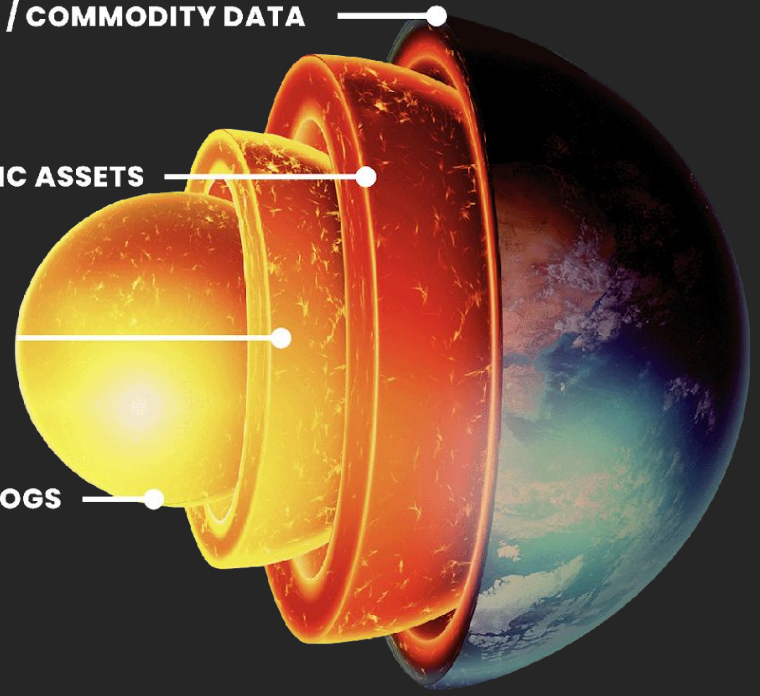
The industry's largest originator of recaptured darknet data

SURFACE
OPEN FORUMS
PUBLIC / COMMODITY DATA

MIDDLE
VETTED FORUMS
DATA STRUCTURED AND SOLD IN SET OF SPECIFIC ASSETS

LOWER
CLOSED GROUPS
DATA TRADED IN TRUSTED CIRCLES

CORE
OFFLINE GROUPS
RECENTLY BREACHED DATA, FRESH BOTNET LOGS



GENERALLY ACCESSIBLE – 80% OF DATA

- Commoditized
- Scanner Sourced but Not Parsed or Actionable
- Occasional Overlapping Access

SPYCLOUD OPERATIONALIZES THESE LAYERS BETTER THAN ANYONE

SPYCLOUD ONLY DATA – 20% OF DATA

- High Value
- Messy & Raw
- Instantly Actionable

ONLY SPYCLOUD HAS THIS DATA DUE TO THEIR BIG DATA APPROACH

DETAILED CREDENTIAL DATA

Where are your exposures?

SpyCloud

Password Reuse for All Time

—

Most Frequently Reused Passwords

Select a single domain identifier to see how many passwords are re-used.

View Exposed Passwords

Exposed Employees

2,519 20% vs last period

Recent Exposed Employees

mcdermott.austin@example.org	Feb 7, 2026
phggoranggriawan@example.org	Feb 7, 2026
phggoranggriawan@example.org	Feb 7, 2026
admin@example.org	Feb 5, 2026
admin@example.org	Feb 5, 2026
admin@example.org	Feb 5, 2026

View Exposed Employees

Infected Employees

493 51% vs last period

Recent Infected Employees

phggoranggriawan@example.org	Feb 7, 2026
mcdermott.austin@example.org	Feb 7, 2026
admin@example.org	Feb 5, 2026
admin@example.org	Feb 4, 2026
antone.conn@example.org	Feb 1, 2026
admin@example.org	Jan 30, 2026

View Infected Employees

Total Records

2,610 24% vs last period

Sources with Highest Record Count

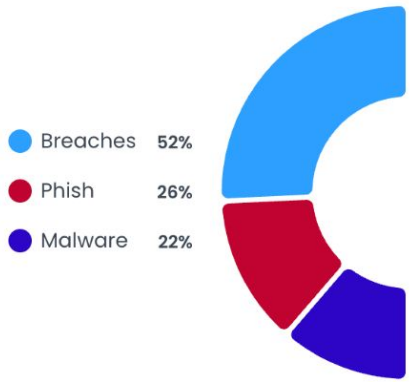
ShaiHulud - The Second Coming	777
Unknown Phishing Kit	668
Ahmadu Bello University Distance Learni...	346
Unknown Windows Stealer	242
LummaC2 Stealer	231

View All Records

Total Sources

327 83% vs last period

Sources by Type



Exposed Assets

53,218

Exposed Assets by Type

PII	25526
Phone	1054
IP	26372
Geolocation	38
Financial	228

Exposed Login Credentials

134,883

Emails
71228

Usernames
13252

Passwords
50403

Latest Active Employee Matches

Automate Compromised Password Remediation

SpyCloud Identity Guardians enable automated remediation of breached, malware-infected and phished directory store accounts directly through Active Directory, Entra ID, and Okta Workforce – safeguarding employee identities and securing access to corporate data and critical IP.

For more information, submit a support ticket and a member from our team will reach out shortly.

DETAILED CREDENTIAL DATA

Where are your exposures?

SpyCloud

Compromised Applications (4310)

Search | Columns | New | Open | Closed

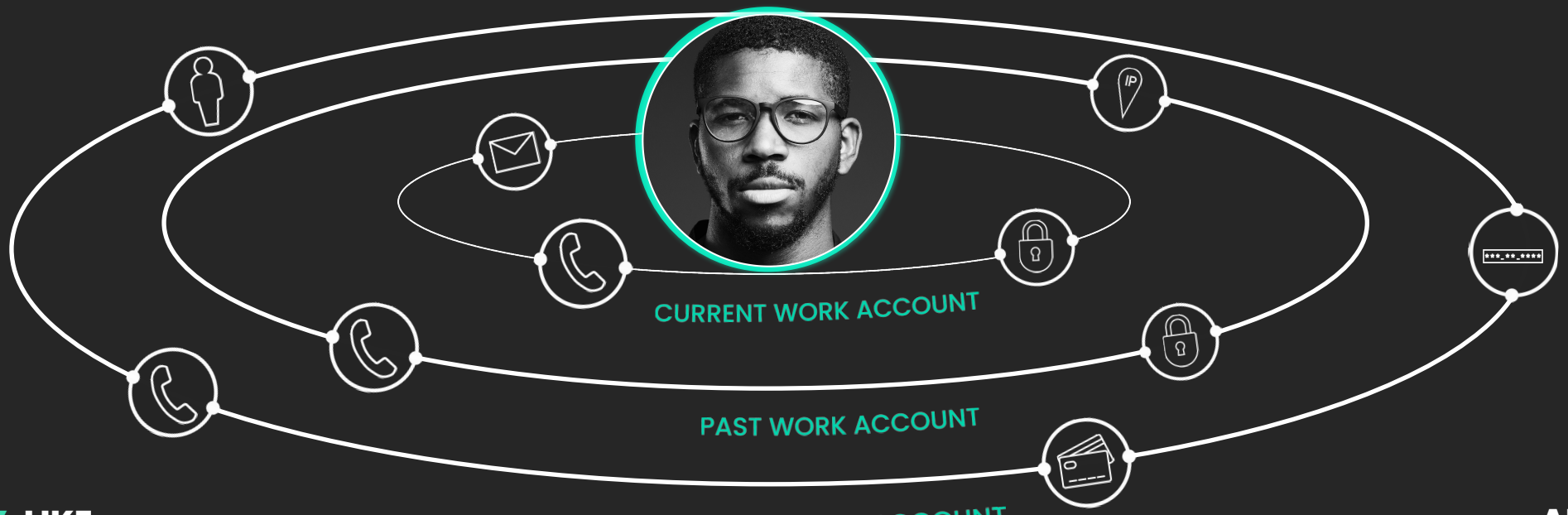
Application	Latest Publish Da...	Emails	Usernames	Compromised Devi...	On Watchlist	Total Records	Cookies	Status
sparefactor.com	12/17/2020	384	0	2,069	Verified	2,069	0	New
hotmail.com	12/17/2020	386	0	2,060	No	2,060	0	New
residential-painting.com	12/17/2020	386	0	1,964	No	1,964	0	New
myspace.com	12/17/2020	384	0	1,949	No	1,949	0	New
gmail.com	12/17/2020	383	0	1,931	No	1,931	0	New
accounts.google.com	2/8/2026	6,573	3,196	1,695	No	15,721	0	New
login.live.com	2/8/2026	2,472	311	1,417	No	4,687	0	New
github.com	2/8/2026	1,123	1,066	1,325	No	3,201	0	New
login.microsoftonline.com	2/8/2026	1,087	56	707	No	2,071	0	New
signin.aws.amazon.com	2/2/2026	956	215	574	No	1,530	0	New

SpyCloud

HOLISTIC DIGITAL IDENTITY

Defining the new standard for identity threat protection

- The most valuable perspective for defending against identity threats – a holistic identity encompasses the full scope of an individual's darknet exposure.
- Well beyond credentials, the holistic identity represents much more than what a company may currently know about an individual employee or consumer that makes the business a target for cybercriminals.



VISIBILITY LIKE YOU'VE NEVER HAD BEFORE

AUTOMATED REMEDIATION TO STOP THREATS

SpyCloud

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
- FINANCIAL THREAT PROTECTION
- FRAUD PREVENTION
- DARK WEB MONITORING

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

CYBERCRIME 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

AUTOMATION ANYWHERE

Rapid remediation to prevent cyber attacks

SpyCloud

1 ANY INTEGRATION YOU NEED, WHERE YOU NEED IT

EDR

- CROWDSTRIKE
- Microsoft Defender

IAM

- Microsoft Active Directory
- okta
- Microsoft Entra ID

SOAR

- CORTEX XSOAR BY PALO ALTO NETWORKS
- Microsoft Sentinel
- splunk>
- tines

SIEM

- splunk>
- elastic
- Microsoft Sentinel
- Chronicle

2 HOSTED AUTOMATION TO ACCELERATE SCALE

SpyCloud Connect builds out custom workflows for your desired integrations without needing to burden your existing resources with custom development work.

YOU → CHOOSE YOUR DESIRED WORKFLOWS AND INTEGRATIONS

SpyCloud CONNECT

BUILDS IT + **MAINTAINS IT** + **SUPPORTS IT**

90 DAYS OR LESS DELIVERY CYCLE

DYNAMICALLY UPDATES IN REAL-TIME

FULLY CUSTOMIZABLE DOWNSTREAM DATA

READY TO DISRUPT CYBERCRIME?

SpyCloud

See why 600+ customers choose SpyCloud

NEXT STEPS:

CONTACT SALES FOR A CUSTOM DEMO

PAYBACK PERIOD	TIME SAVINGS	IDENTITIES PROTECTED
3.5	**~60%**	**4B+**
MONTHS	**TIME SAVED**	**ACCOUNTS**
AVG PAYBACK PERIOD	LENDINGTREE SOC TEAM	PROTECTED GLOBALLY

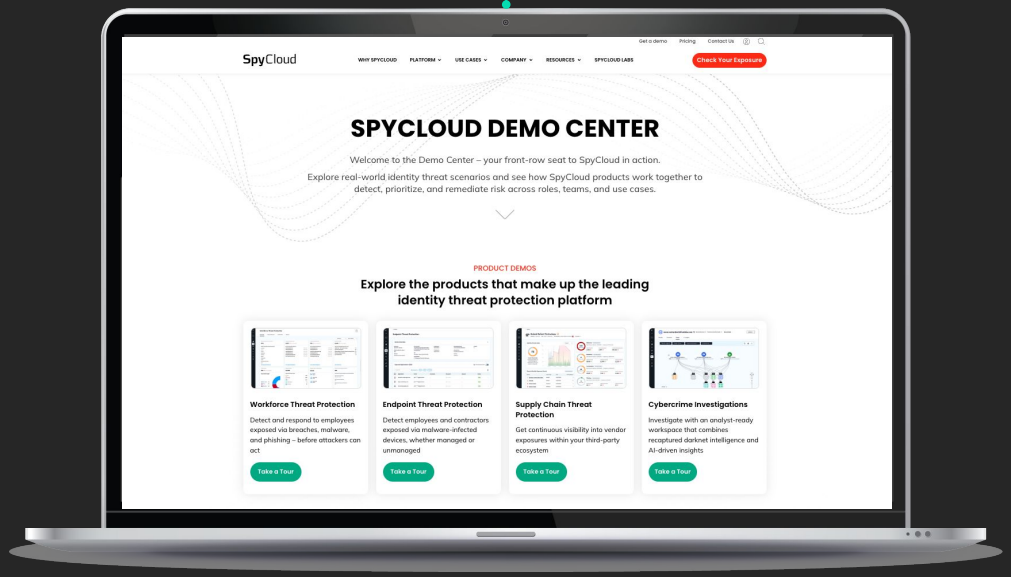
ADDITIONAL RESOURCES

SpyCloud

SEE MORE

SPYCLOUD DEMO CENTER

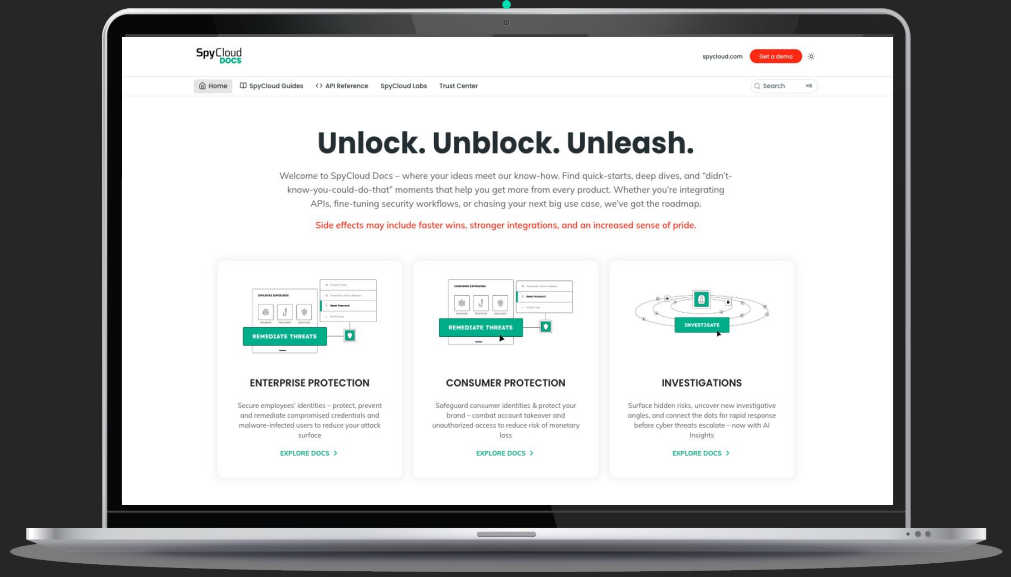
Your front-row seat
to SpyCloud in action



KNOW MORE

SPYCLOUD DOCS

Technical documentation for building,
integrating, & operationalizing SpyCloud



RSAC | 2026 Conference

San Francisco • March 23 – 26 • Moscone Center

SpyCloud

SEE WHY SPYCLOUD IS THE LEADER IDENTITY THREAT PROTECTION

BOOTH #S-3338

SpyCloud
THANK YOU