BUYERS GUIDE

SpyCloud

ENTERPRISE PROTECTION

GUIDE TO

Protecting Against Next-Gen Threats

BUYERS GUIDE

WHAT'S INSIDE

PEOPLE ARE THE NEW PERIMETER

Digital identities are the foundation of our modern lives, but they are continuously vulnerable to threats. To stay ahead, security teams need to stop swimming in threat intel data feeds - they need to get clarity and take action with **an identity-centric approach**.

People – employees, third-party vendors, and customers – and their expansive digital identities have exponentially multiplied entry points for attacks on organizations. Criminals are exploiting these gaps through account takeover and follow-on attacks, fueled by authentication data stolen from third-party breaches and malware. As your organization adapts its defenses accordingly, you may be looking for tools to layer into your existing security stack.

There's no better time than now to prioritize targeted and emerging forms of account takeover and ransomware prevention – but to do so, you need to be able to act on what criminals have in hand before they do. **SpyCloud offers an approach that's more comprehensive and actionable than traditional threat intelligence;** powered by analytics that connect compromised entry points to employee identities and giving security teams a seamless integration to automatically remediate the threat.

ACCESS IS THE NEW CURRENCY FOR CYBERCRIMINALS

The definition of a credential has evolved, and it's no longer just about your password. Each authentication layer in your network serves as a credential – broadening the scope in which criminals can bypass security measures to gain access with just a few clicks.

How we think about threat intelligence needs to change – in terms of what we collect and how we process and take action on that information. Addressing rising cybercrime trends and tactics is essential in proactively safeguarding the digital identities of your workforce and protecting the integrity of your corporate data.

44+ BILLION
stolen device & session cookies recaptured by SpyCloud

81%
of organizations were affected by ransomware in 2023

The best defense is to secure your people. Doing so requires a shift from a device-centric view of detection, prevention, and response to one that encompasses the full employee identity.

WHERE TRADITIONAL THREAT INTEL FALLS SHORT

Historically, threat intelligence is good at providing broad context about your security environment to understand threats, but leaves you swimming in data, whereas SpyCloud gives you definitive evidence of compromise - AND the lever to do something about it.

- Typically, threat intel feeds scrape pretty much everything and anything. This becomes draining as teams work to manually sort and sift through data to uncover meaning and correlate risk.
- Threat intel scrapes data in mass quantity, often riddled with false positives, which overloads analysts trying to validate indicators of employee compromise.
- Traditional threat intel relies heavily on OSINT or publicly-sourced data, which savvy criminals have already monetized.
- Traditional threat intelligence is often retrospective and becomes stale quickly. This reactive approach hinders automation initiatives to prevent attacks.

MAKE INFORMED DECISIONS WITH CYBERCRIME ANALYTICS

Cybercrime Analytics (C2A) is the new way to disrupt cybercrime. SpyCloud leverages a highly advanced and scalable process of ingesting and normalizing unstructured breach and malware-exfiltrated data. The outputs are actionable insights enterprises can use to prevent cyberattacks, safeguard employee identities, and swiftly investigate exposures.

SpyCloud's analytics are based on industry-leading, continuously-updated recaptured data, with more than 240 unique data types including:

24B+
CRACKED, PLAINTEXT PASSWORDS

33B+
EMAIL ADDRESSES

1B+
MALWARE RECORDS

44B+
STOLEN COOKIES

ABOUT SPYCLOUD ENTERPRISE PROTECTION

SpyCloud empowers security teams to rapidly respond to exposed credentials and proactively prevent evolving threats to employees and corporate data. SpyCloud's **Enterprise Protection** layers into your existing tech stack with seamless integrations with security tools you're already using, and scales with the threat landscape – backed by analytics derived from the industry's largest repository of recaptured data.

In this guide, you'll learn how SpyCloud enhances four critical aspects of cybersecurity defense to safeguard your employees' identities and sensitive data against next-generation cyberattacks:

- **MONITORING & DETECTION** | Continuously monitoring employee identities to detect exposed authentication data
- **ATTACK PREVENTION** | Preventing the takeover of compromised accounts and minimizing targeted risks by identifying exposed sensitive data early
- **TURNING INTEL INTO ACTION** | Providing truly actionable data to inform your response, alerting, and investigation procedures
- **DYNAMIC AUTOMATION** | Automating key parts of your security practices to fuel a prompt and effective response

THE POWER OF SPYCLOUD

SpyCloud Enterprise Protection safeguards employees' digital identities – delivering a solution that continuously monitors for compromised credentials, keeps corporate data safe, and reduces overall enterprise risk. With actionable analytics, security teams can extend automated protection across their organization while optimizing response and remediation efforts for proactive coverage against targeted attacks.

1 Monitor and Detect, Beyond the Password

We understand that an employee's digital identity is comprised of much more than just a password. SpyCloud Enterprise Protection offers an inclusive that spans an employee's entire digital footprint – proactively detecting and remediating exposures to prevent unauthorized access and stop next-gen attacks before they happen.

GET A COMPREHENSIVE VIEW OF DARK WEB ASSETS

SpyCloud secures employee identities with insights into all stolen data from breaches and malware-infected devices, including user credentials, cookies (or sessions), and high-value PII. This data is used by criminals to impersonate users for targeted account takeover.

DETECT ACTIVE THREATS EARLY

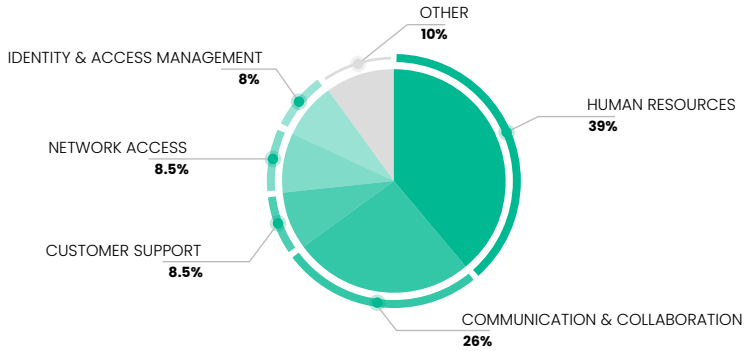
SpyCloud enables rapid detection and response times – continuously monitoring for exposures to identity risk early and shorten the time between exposure and criminal exploitation. SpyCloud gives you the needle, without the haystack - surfacing exposures both before they've hit readily accessible public forums and before legacy threat intel providers. Armed with exact-match technology, security teams can reset exposed credentials before criminals can act.

DETECT THREATS REGARDLESS OF DEVICE

Criminals are increasingly turning to infostealers to steal credentials. SpyCloud offers a device-agnostic approach – detecting malware exposures that affect employee applications, regardless if the infection occurred on the work, home or mobile device.

DETECT HIDDEN EXPOSURES TO CORPORATE APPLICATIONS

SpyCloud removes blindspots into unauthorized access to business applications via malware-exfiltrated credentials, even from third-party vendors and contractors accessing your network from compromised personal or undermanaged devices. Credentials exposed to third-party SaaS applications (like Okta or Atlassian, and even Slack) could serve as entry points to employee account takeover.



▲ SpyCloud's ongoing analysis of malware infections reveals which popular business tool categories are most frequently exposed

KEY SPYCLOUD CAPABILITIES

SaaS PORTAL

Secure access to a portal where security teams can view breach and malware exposures

ADMIN CONTROL

Admins can add or remove domains, email addresses, and IP addresses to the SpyCloud Watchlist for customized monitoring

GRANULAR ATTRIBUTION

Rich context and correlation of compromised data sources to decrease dwell time and enable rapid response

2 Prevent Targeted Cyberattacks by Reducing Entry Points

Preventing targeted cyberattacks requires more than just monitoring and detecting. Teams need a full understanding of how criminals are using data to sidestep authentication and take control of employee accounts. Here are four ways SpyCloud advances your attack prevention strategy:

OPTIMIZE PASSWORD POLICIES

Poor password hygiene and lax governance are leading causes for employee account takeover. SpyCloud helps you comply with NIST guidelines for **enforcing password requirements in Active Directory** regarding length, complexity, and uniqueness. In addition, SpyCloud lets you configure a list of banned passwords in Active Directory to prevent employees from using your custom list of terms, like company name and sports or pop culture references. If SpyCloud detects a match on banned or previously-exposed passwords, the risky password is blocked.

PREVENT PASSWORD REUSE

Regularly monitoring for password reuse prevents lateral attacks and allows you to identify employees at risk for targeted account takeover. SpyCloud runs scheduled scans of your Active Directory passwords against our repository of exposed credentials to identify when passwords are in the hands of criminals. SpyCloud catches exact-match exposures of compromised passwords in near real-time, and immediately takes action to shut down this entry point.

PREVENT AUTHENTICATION BYPASS

Infostealer malware-siphoned session cookies allow bad actors to bypass all forms of authentication, even SSO on trusted devices, enabling lateral access across the network. SpyCloud delivers compromised cookie data associated with your domain, including the information you need to identify which employee accounts are vulnerable and take your desired action.

PREVENT EXPOSURE ACROSS YOUR SUPPLY CHAIN AND EXECUTIVES

Criminals often target VIPs. SpyCloud extends your account takeover prevention strategy to the personal accounts of executives, board members, and even developers with systems access – to detect exposures that may act as entry points for follow-on attacks. SpyCloud also monitors the third-party domains of your supply chain vendors to identify threat exposure from exposed individuals who may have privileged access.

KEY SPYCLOUD CAPABILITIES

CUSTOM REMEDIATION POLICIES

Options include notifying users with custom emails sent from a known address, disabling users, or applying to users based on role

NIST COMPLIANCE

Align to NIST password guidelines by preventing employees from setting weak or compromised passwords and automatically filtering out bad passwords

EXECUTIVE REPORTING

Get high-level reports with exposures and corresponding account takeover prevention outcomes to share with executive leaders

3 Drive Results with Next-Gen Intelligence

Traditional threat intel becomes stale quickly, generating too much noise and resulting in not enough action, putting a strain on your resources. SpyCloud provides high-fidelity alerts that empower teams to make confident decisions – easily integrated into your existing workflows and accelerating automation efforts within your organization. Here are four ways SpyCloud drives meaningful results:

- **CURATED DATA TO REMOVE NOISE**
  SpyCloud parses and normalizes over 240+ distinct attributes of recaptured darknet data. We focus on high-value information like employee credentials, discarding duplicates to prevent noise from hitting your SIEMs.

- **ENRICHED DATA FOR ACTIONABLE INSIGHTS**
  SpyCloud enhances recaptured data with contextual details including source and breach description along with the password. Over 90% of our published passwords are plaintext, allowing for exact matches with active employee credentials. For malware records, we provide comprehensive context including the IP address, infection details and path, along with target URLs, credentials, and cookies for applications, so you can fully remediate the exposure.

- **ROBUST CORRELATION TO MITIGATE EXPOSURES**
  SpyCloud's analysis goes beyond traditional device-level remediation by connecting employee identity credentials across breaches and malware infections. This holistic view, enriched with insights like OS, IP address, and location, shortens investigation time and enables your team to accurately prioritize and respond based on the full scope of employee exposure.

- **ADAPT TO EVOLVING CRIMINAL TACTICS**
  SpyCloud's ever-expanding collection of recaptured data types scales with the latest trends in exfiltrated malware data due to SpyCloud Labs, our dedicated security research arm. This deep understanding of the criminal ecosystem means you're able to stay ahead of evolving threats before they become mainstream, with insights into stolen session cookies, API keys, password vaults, and more.

SC LABS

SpyCloud Labs is a dedicated research team that is relentlessly focused on analyzing active tactics seen in the criminal underground so that our solutions can be enhanced by the evolution of these threats.

KEY SPYCLOUD CAPABILITIES

DATA EXPORT
Export anything as a CSV to enable your desired level of analysis and create custom reports based on individualized or use case metrics

INTERACTIVE GRAPHS
Visualizations show the scope of a potential threat, including infected devices, users, and applications with actionable details

HIGH-FIDELITY ALERTS
SpyCloud provides detailed evidence that stolen data tied to your enterprise is in criminal hands and alerts you of new exposures

4 Scale with Automated Response

Everyone is looking to trim down on heavy and manual investigative work. Security teams can accelerate the scale of their operations and respond rapidly to identity threats through seamless automation. SpyCloud's extensive set of integrations with key vendors across the entire security landscape delivers actionable, next-gen intelligence to power your efficient response against next-gen threats.

INTEGRATE PROTECTION WITH IDENTITY BROKERS

Start with SpyCloud to safeguard employee identities via integrations into leading directory services, whether on-prem, hybrid or cloud-based, as well as leading Identity Access Management brokers like Okta. SpyCloud's integrations scan for any risks of active employees using compromised passwords at login or exposed application credentials. You can force password resets if SpyCloud detects a match against our dataset, or go further to disable accounts to prevent targeted ATO.

INTEGRATE HIGH-FIDELITY ALERTS INTO SIEMS

SpyCloud feeds breach and malware records continuously into leading SIEM solutions as high-fidelity alerts so your teams can efficiently prioritize and escalate actions to the relevant personnel. By surfacing only the most critical issues, SpyCloud's alerts drive productive investigations to shorten the attack window.

AUTOMATE SOAR REMEDIATION

SpyCloud streamlines incident response with pre-built playbooks for major SOAR vendors, enabling efficient response to breaches and high-priority malware exposures. New incidents are automatically created within your workflows for exposed passwords for business application credentials, which can trigger additional steps to help automate the remediation of the affected users and devices.

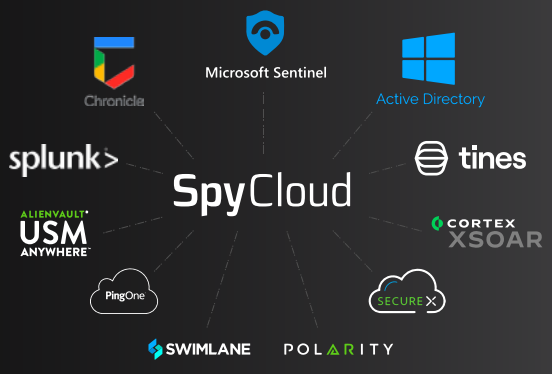
AUTOMATE ADVANCED WORKFLOWS WITH SPYCLOUD'S DATASET

The integrations between SpyCloud and SIEMs and SOARs enable querying SpyCloud's API to retrieve additional enriched records within our database. You can use any critical indicators of employee exposure to develop custom automation steps within your broader security ecosystem for streamlined incident response. Think of the efficiencies gained by orchestrating workflows across other security tools using SpyCloud exposure records, improving collaboration via Slack or MS Teams, or automatically creating tickets in ServiceNow or Zendesk.

KEY SPYCLOUD CAPABILITIES:

Out-of-the-Box API Workflow Integrations

Integrate SpyCloud breach and malware alerts with common SIEMs, SOARs, and ticketing platforms to automate response and prevent employee account takeover. Trigger alerts in internal detection software to optimize incident response processes. With our integrations, you can automate:



TRIAGE & ESCALATION ▪ **INCIDENT RESPONSE WORKFLOWS** ▪ **POST-INFECTION REMEDIATION**
ACCOUNT TAKEOVER & RANSOMWARE PREVENTION ▪ **INVESTIGATIONS OF ANOMALOUS ACTIVITY**

HOW TO IMPLEMENT SPYCLOUD ENTERPRISE PROTECTION

SpyCloud Enterprise Protection layers into your existing security operations with minimal overhead.

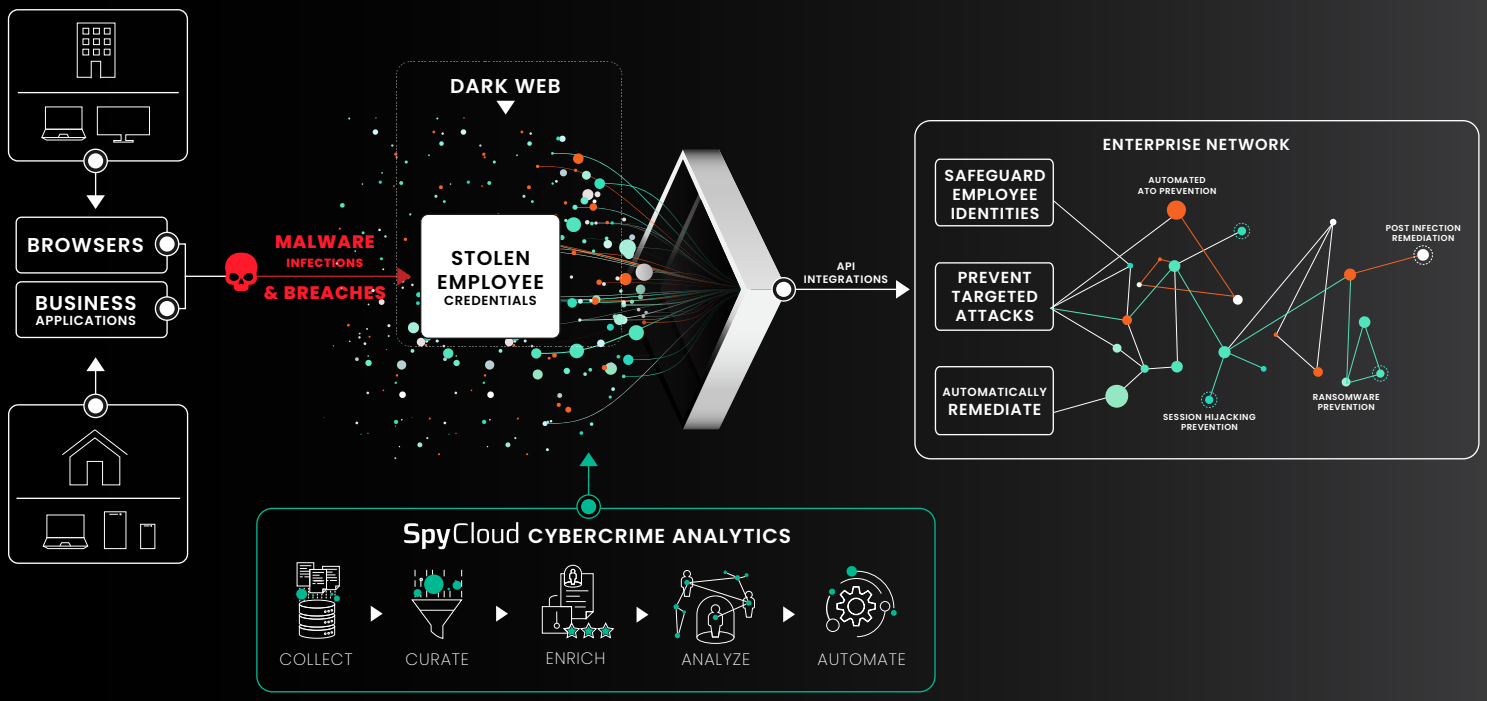
- **INTEGRATE INTO SOC WORKFLOWS |** Integrate actionable, flexible, and consolidated Cybercrime Analytics into your SOAR/SIEM to accelerate the remediation of compromised credentials and malware-infected devices, users, and applications.

- **LAYERED ALERTING |** SpyCloud's high-fidelity alerts are published across various channels, including SpyCloud's portal, via scheduled emails, or directly via the API. You can layer the alerting into your preferred communication channel and frequency.

- **LAYERED DEFENSE ACROSS ENTIRE OPERATIONS |** SpyCloud's solution layers defense for employee accounts, your executives' and VIPs' personal lives, and into your critical supply chain.

- **LAYERED INTELLIGENCE FOR MULTIPLE TEAMS |** SpyCloud's Cybercrime Analytics power detection, prevention, remediation, and automation. Teams ranging from SecOps to CTI, or across departments like Identity, benefit from this actionable data to protect employee identities and your corporate data.

SpyCloud's Cybercrime Analytics tie exposures from breaches and malware infections to your employees' identities, and automate action via integrations with your enterprise network for better security outcomes.



ENTERPRISE PROTECTION PRODUCT SUITE

SpyCloud product licensing is offered as tiered pricing by the number of employee accounts protected.

COMPASS
Protect your company from ransomware and other critical threats with Post-Infection Remediation.

EMPLOYEE ATO PREVENTION
Protect your company from ATO, data breaches, and BEC resulting from third-party breach exposures.

ACTIVE DIRECTORY GUARDIAN
Automatically reset accounts exposed in third-party breaches and malware infections. Trigger SSO credential resets with Okta.

THIRD-PARTY INSIGHT
Monitor supply chain ATO risks and share data with partners to aid remediation.

SESSION IDENTITY PROTECTION
Prevent unauthorized access of critical workforce services including SSO.

VIP GUARDIAN
Empower your highest-risk employees to secure their online identities without sacrificing privacy.

> ***SpyCloud have been great to work with, their customer engagement and support is excellent and the quality of their data is top notch and actionable. When ever we get an alert from them we always follow it up as it is always fresh intel."***

Gartner Peer Insights

WHY CUSTOMERS CHOOSE SPYCLOUD

- **DEEPER, DARKER, BETTER |** Faster access to recaptured data for swift action. Context-rich data beyond the breadth and depth of threat intel providers, with data highly relevant to your organization.
- **ACTION-DRIVEN ANALYTICS |** Alerts that you want more of to save time on tedious discovery and correlation. SpyCloud alerts are valuable to your teams to shorten the investigation time, without manually correlating or de-duping the data, to only deliver exposed credentials that truly pose risk.
- **AUTOMATION & EXTENSIBILITY |** Scales with the threat landscape, protecting you today and tomorrow. A growing amount of recaptured data published frequently alongside extensive integrations across multiple categories of security tools that you're already using, to support your existing automated workflows.
- **LAYERED INTELLIGENCE |** Coordinated response across teams and within your existing security framework doesn't force you to rip and replace your existing security framework. Layer in SpyCloud's analytics into your existing practices for a coordinated response to maximize impact with minimal organizational overhead.

KEY OUTCOMES

Saves **60% of SOC team's time and resources** with actionable data & automation

Protects **1,000 employee accounts** & **millions of customer accounts** from ATO and ransomware

Supports organization-wide **security posture & brand integrity**

Reduces alert fatigue with high-fidelity notifications

"I know if I get a SpyCloud alert, it's actionable ...

We consider SpyCloud as a trusted resource for any type of incident that may impact our consumers or employees"

—

Anthony Brunson

SECURITY OPERATIONS MANAGER, LENDINGTREE

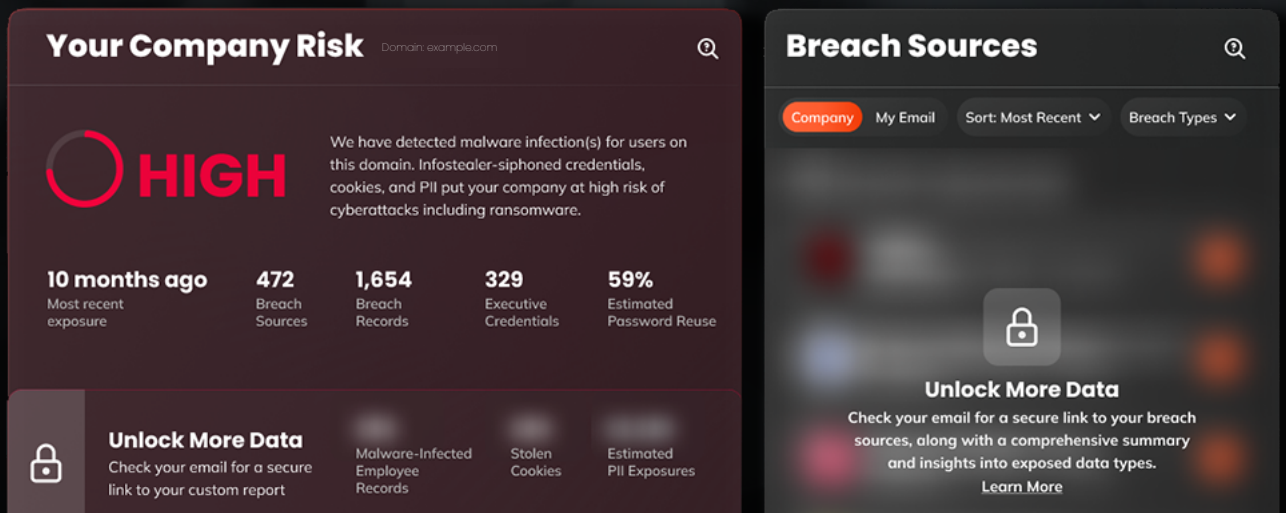
READY TO PROTECT YOUR DIGITAL PERIMETER WITH SPYCLOUD?

SpyCloud enhances critical aspects of your security defenses to safeguard your sensitive data against next-generation cyberattacks. To get a glimpse into the power of Cybercrime Analytics, start by checking your enterprise exposure. We'll reveal real-time insights on exposed employee credentials that are in the hands of criminals and share the results – including any previously unknown exposures that SpyCloud illuminates – in a custom report.

Your custom exposure report includes:

- **An overall security risk score for your business based on SpyCloud's data, taking into account malware infections and plaintext passwords**
- **A count of malware-infected records associated with employee email addresses, which may indicate active infections and exposed active session cookies**
- **Insights into third-party breach records, exposed executive and VIP credentials, estimated password reuse, and PII exposure for your employees**
- **Specific breach and malware sources, with details on when SpyCloud published the data to customers and compromised data types**

GET MY REPORT ››



THE SPYCLOUD COMMITMENT TO CUSTOMER SUCCESS

Success from day 1

Our technical account managers work with you for a smooth onboarding process to align on your desired outcomes.

Ongoing optimization

Your dedicated customer success manager will provide ongoing support at regular cadences to maximize your investment and discuss SpyCloud's ability to help with other security initiatives.

Online chat

We offer global support and responses within 24 hours for any issues that arise during navigating our portal, calling our APIs, or responding to recaptured data.

ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to protect businesses from cyberattacks. Its products operationalize Cybercrime Analytics (C2A) to produce actionable insights that allow enterprises to proactively prevent ransomware and account takeover, safeguard employee and consumer identities, and investigate cybercrime incidents. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to make the internet safer with automated solutions that help organizations combat cybercrime.

To learn more and see insights on your company's exposed data, visit **spycloud.com**.