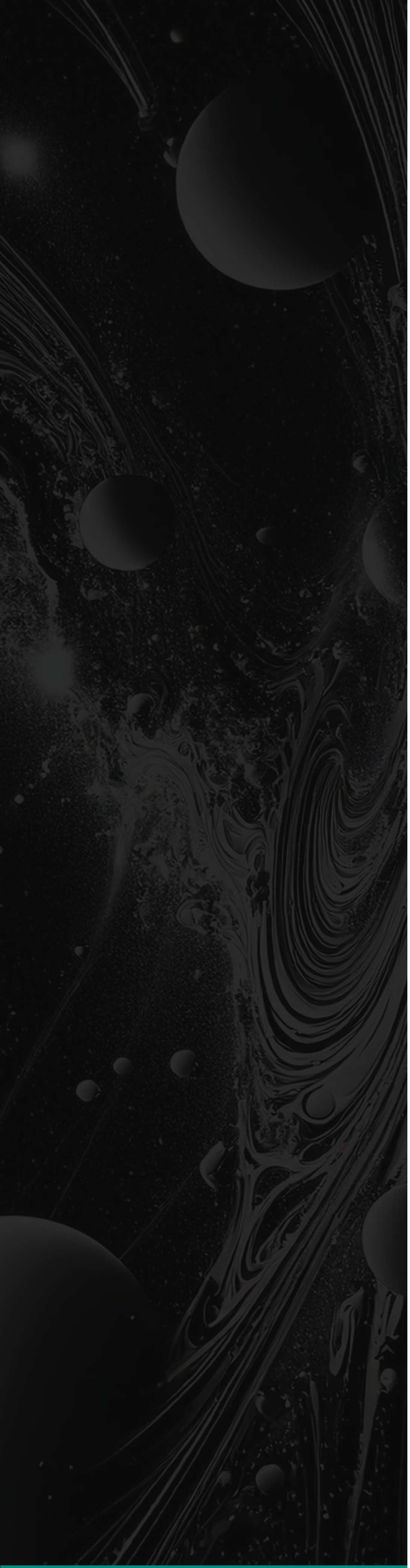
THE HOLISTIC IDENTITY FRONTIER

The shift from account-centric security to holistic identity threat protection

SpyCloud

WHAT IS A HOLISTIC IDENTITY?

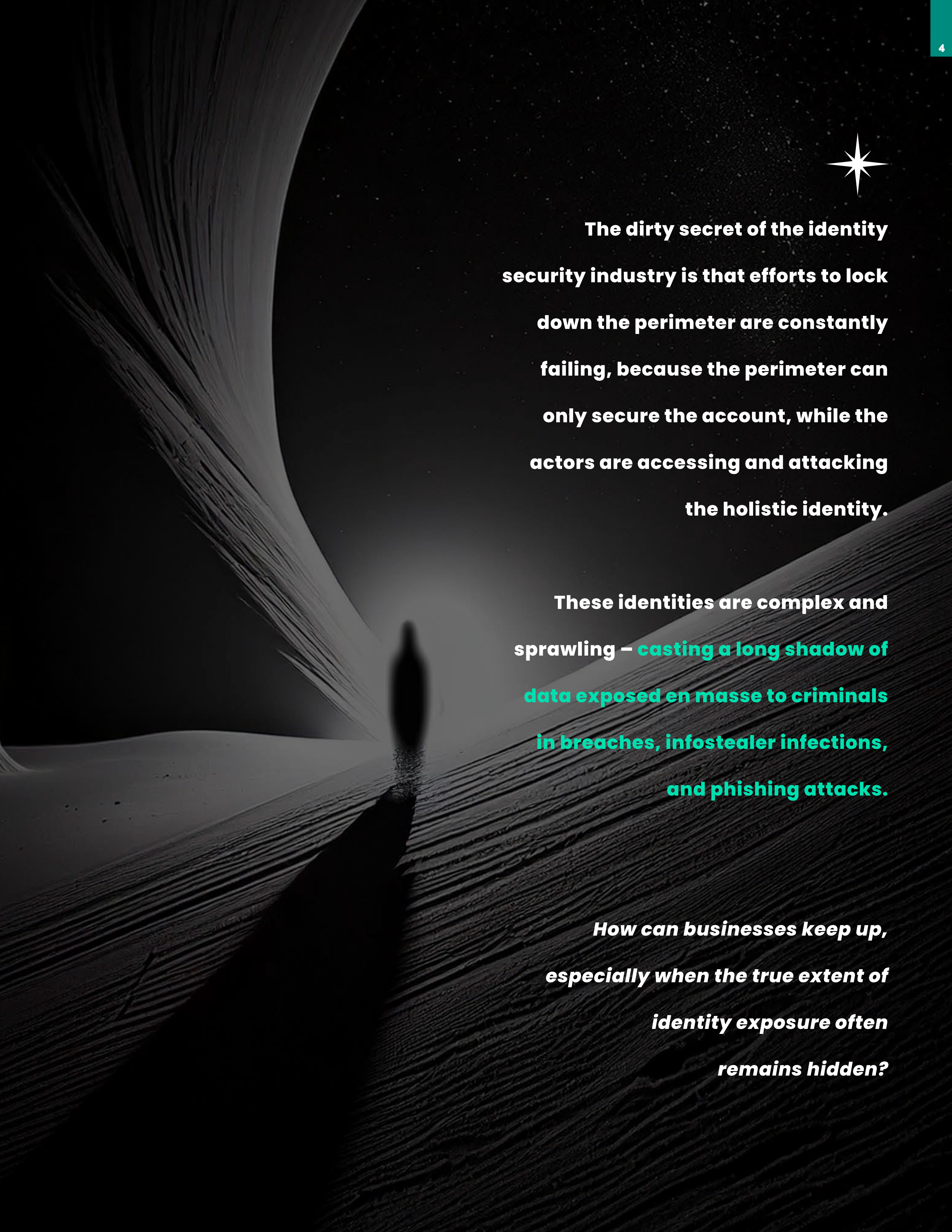
The most valuable perspective for defending against identity threats **– a holistic identity encompasses the full scope of an individual's darknet exposure.** Well beyond credentials, the holistic identity represents much more than what a company may currently know about an individual employee or consumer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



FOR THE LAST FIFTEEN YEARS...

the security industry has invested heavily in protecting “identity as the new perimeter.” Billions of dollars have been spent on defining and protecting corporate identity accounts, machine identities, and consumer identity accounts. Entire industries have been built around protecting each of these core identity elements, including Identity and Access Management (IAM) and Identity Threat Detection & Response (IDTR).

Unfortunately, every existing solution is bound by the reality that each company is limited by the data that they can collect, based on their own infrastructure – but criminals do not have these same boundaries. While businesses are limited to the user details and access patterns of each user account, bad actors go way beyond that account, harvesting everything they can from the online lives of each employee, customer, partner, and supplier, accessing darknet areas that have been trading in illicit identity data for decades.



The dirty secret of the identity security industry is that efforts to lock down the perimeter are constantly failing, because the perimeter can only secure the account, while the actors are accessing and attacking the holistic identity.

These identities are complex and sprawling – casting a long shadow of data exposed en masse to criminals in breaches, infostealer infections, and phishing attacks.

How can businesses keep up, especially when the true extent of identity exposure often remains hidden?

RIGHT NOW...

most teams are trying to tackle the problem by addressing the stolen identity data they know about – what they get from threat intel feeds, for example, or the incomplete, commoditized, and stale data that in-house teams are able to find via open source solutions. That data is typically limited to stolen credentials for individual accounts from a limited collection of breaches, and doesn't connect the dots to give you a true picture of user compromise that you can act on to confidently protect your business.

Even with access to limited data feeds and highly scaled out IAM solutions, criminals are still logging into enterprises.

The use of stolen identity information remains the leading initial action in **24% of data breaches**

Compromised credential attacks result in **$4.81 million in related costs per breach** and take the longest to identify and contain

SpyCloud's own data recapture in 2024 alone delivered more than **8B stolen identity records** to enterprise security teams

And even with huge investments in IAM, ITDR, MFA, FIDO, and additional identity technologies, we are still seeing massively successful and costly identity attacks. This is because the criminals are playing on a much larger field than enterprises.

To truly protect your enterprise, you must act with knowledge of users' holistic identity exposures across their many online personas, personal and professional, because they all impact your business – you just can't fully visualize or act on them right now with your existing tools. As a result, you're likely only able to remediate specific account exposures, which represent mere fragments of identities, and not on the more comprehensive data criminals are using now to target your business.

The shift from account-centric security to holistic identity threat protection allows you to enter the real game that criminals are playing and will have a dramatic effect on your cyber and fraud risk mitigation strategies.

This paper defines how a holistic identity-centric approach to cyber threat protection differs from traditional security approaches, along with its use cases and benefits in detail. By the end, you'll understand how a holistic digital identity lens based on exposed darknet data, enriched insights, and automated workflows will allow your team to act on more exposures than ever before, and resolve issues that have plagued security teams since the dawn of passwords, illuminate potential insider threats, enable attribution faster, and effectively change the game in your favor.

THE HOLISTIC IDENTITY

If you're still thinking about 'identity' as it's defined now, your framing is about a distinct and individual digital representation of a user, device, or entity within your network and systems. This digital identity comprises attributes that uniquely define and authenticate each entity and control its access to resources.

The concept of a holistic identity is additive and takes a broad point of view to answer several questions:

- ***What data about an individual is in criminal hands?***
- ***How many online personas are represented in that one individual's identity?***
- ***What data that may expose the enterprise is hidden or unknown – but connected to the corporate identity with advanced analysis?***
- ***How can all this data be correlated and surfaced to security teams to take action and make decisions based on reused passwords, stolen cookies, exposed PII, and more?***

A holistic identity is a view of exposed data from breaches, malware infections, and phishing attacks, correlated to an individual across their many online personas. The individual in question may be a current or past employee, consumer, partner, or supplier, but their exposed identity data presents a risk to the business in some way, via access to corporate systems, or sensitive customer or financial data that can facilitate data breaches, BEC, account takeover, session hijacking, ransomware, and fraud.

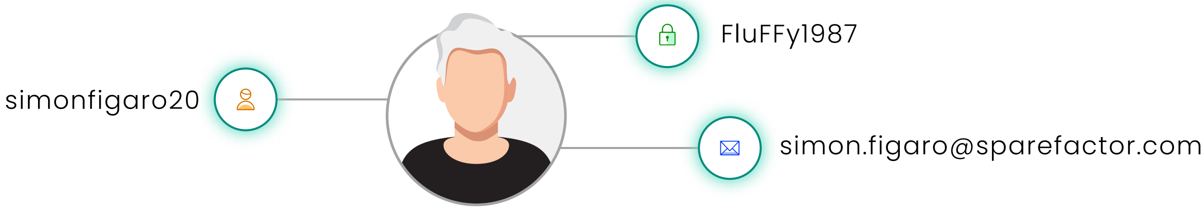
While the holistic identity of a user absolutely extends beyond darknet data, since underground data is what criminals use to fuel these costly and damaging cyberattacks, **it is the most valuable perspective for defending against identity-based cybercrime**.

With the blurred line between personal and professional online personas, the ability to understand identities holistically has become increasingly urgent – and it's now in the purview of security teams to detect and remediate exposures from holistic identities in order to better protect their business.

THE AVERAGE USER IDENTITY

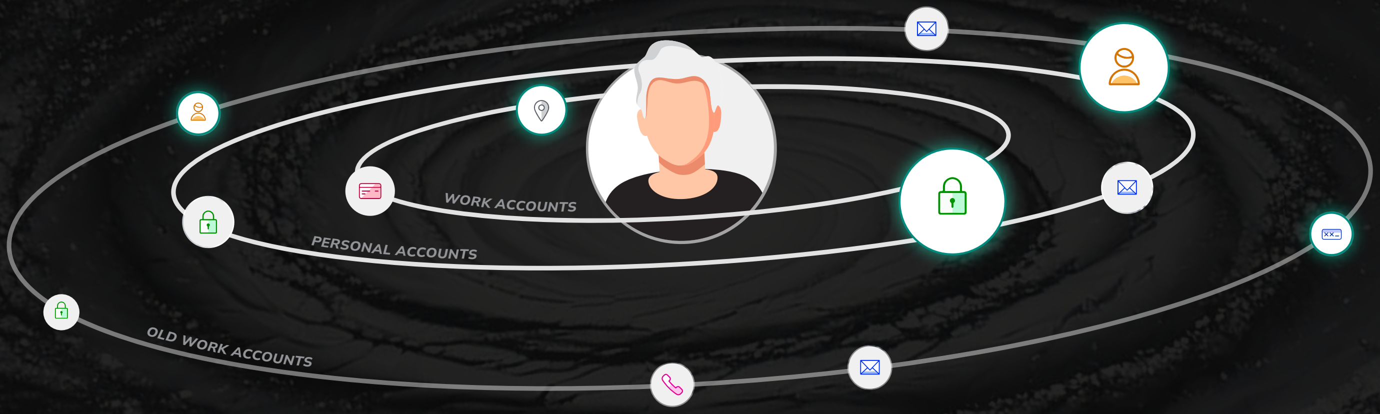
ACCOUNT-CENTRIC APPROACH

Simon Figaro



HOLISTIC IDENTITY APPROACH

Simon Figaro

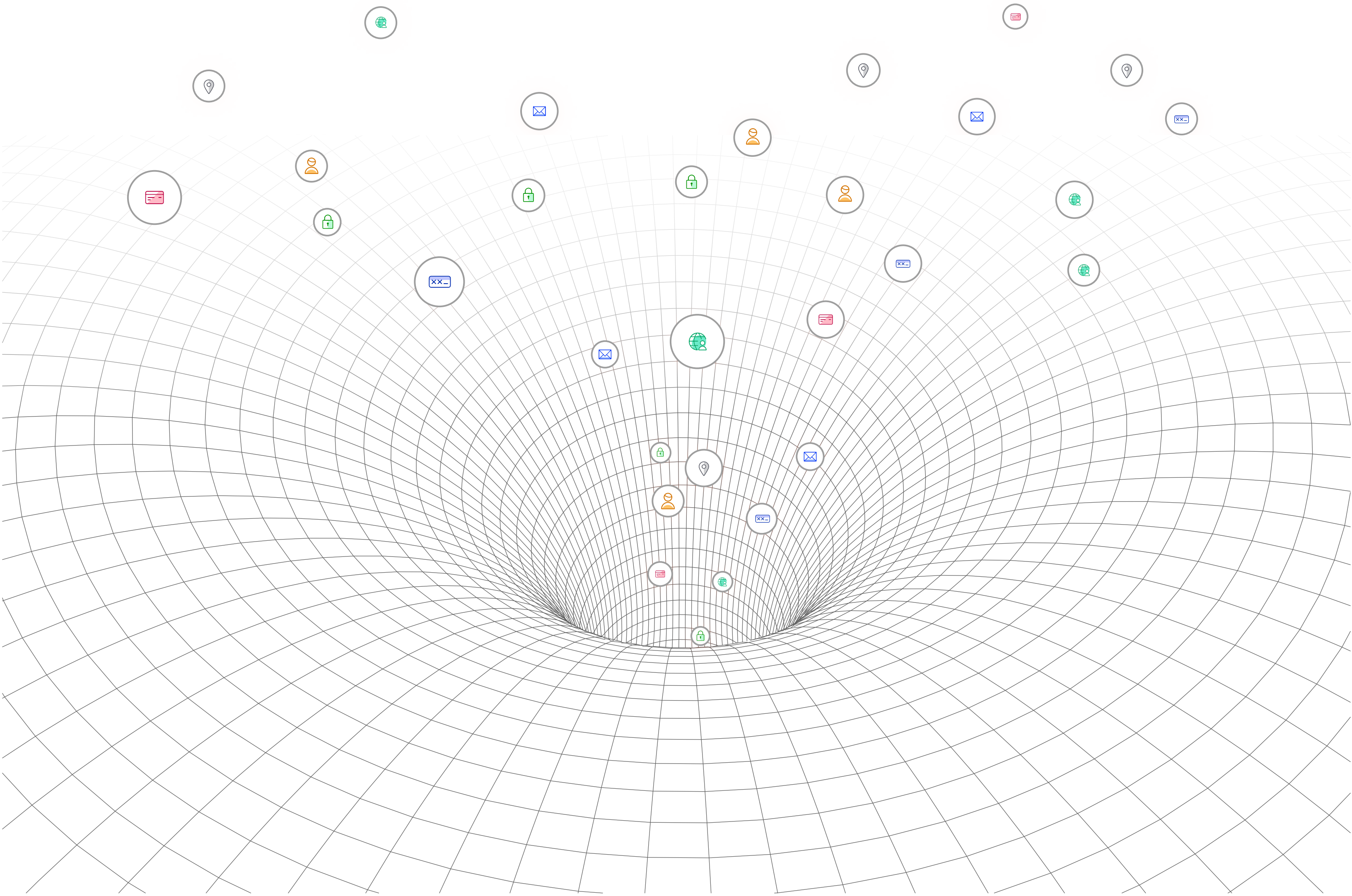


SpyCloud

Given SpyCloud's vast database of nearly 50,000 recaptured breaches, malware victim logs, and phished data, its holistic identity lens reveals an interconnected web of darknet-exposed information that's both highly desirable to criminals and imperative for businesses to understand:

- **Credentials**: Email addresses, usernames, plaintext passwords, passkeys, session cookies, API keys
- **PII**: Full names, home addresses, phone numbers, dates of birth, SSNs or national ID numbers, passport data
- **Financial data**: Credit cards, bank accounts, crypto wallet addresses
- **Other sensitive information**: Social handles, IP addresses

Incorporating holistic identity threat protection into your cybersecurity and fraud prevention programs means you can ***protect your business from previously hidden identity assets and reduce unseen risk*** like never before possible.



WHY SPYCLOUD

At SpyCloud, we've spent nearly a decade surfacing identity exposures and facilitating rapid, automated remediation to prevent fraud for **businesses large and small**. We've harnessed the knowledge of renowned cybercrime investigators and researchers on our team, including former intelligence agency personnel, about how threat actors think and evolve. And we've used that expertise to infiltrate criminal communities to recapture and share with defenders the same data criminals know about their business, their customers, and their supply chain – the same data criminals are actively using for their next attack.

But we know it now takes more than this. Our customers know there are threats they can't see, and they can't react to the things they don't know about. With **attacks surging** in the wake of major leaks like the **National Public Data Breach**, we are seeing the risks of identity-based attacks multiply before our eyes – but luckily, we've kept pace.

As we've built and maintained the largest, richest darknet data lake, we've also applied leading data science to refine our analytics engine to dynamically correlate billions of datapoints to reveal a bigger and more accurate picture of identities. Through proprietary technology built on our deep big data expertise, we can instantaneously tie together the threads of common authentication data and PII – think shared passwords across seemingly unrelated usernames but with connected IP addresses and phone numbers – continuously and at scale. We've refined the outputs and validated them with customers and external working groups who are already seeing the value in this approach.

SPYCLOUD IS INTENSELY FOCUSED ON IDENTITY THREAT PROTECTION

This is the automated remediation of the threats brought to your enterprise by the holistic identities being tracked and traded by criminals on the darknet.

We know that this starts with the quality and depth of our exposure data – collected and enriched over time by SpyCloud Labs, the leading minds in security research and tradecraft. But the data alone is not enough; we've applied industry-leading data science expertise and automated analytics to drive insights and correlations to truly understand the threats our customers face. With a robust ecosystem of out-of-the-box and customized integrations, SpyCloud makes acting on high severity exposures easy and tailored to your preferred toolset.

In doing so, our holistic identity analysis of 2024 stolen personal data shows:

- The average individual has many as **52 unique usernames/emails and 221 passwords connected to their identity**, via exposures of their various online personal and professional personas.
- **Three out of four individuals that had personal data stolen** were victims of an infostealer malware infection, which exfiltrates, on average, dozens of account credentials and myriad PII from affected devices.
- **90% of individuals have at least one exposed IP address**. Exposed IPs enable criminals to mimic trusted IP addresses from victims' home locations to bypass location authentication measures to commit crimes, especially fraud, by obfuscating their identity and location.

These findings should send a chill down the spine of anyone responsible for stopping identity threats.

We all know users are the weakest link in any security program, but defenders can only take action if they know what has been compromised. And while security teams know a lot – their privileges, their activities on corporate systems, their normal and anomalous user/device behaviors, MFA failures, leaked credentials, and risks associated with their endpoints – **they can't remediate what they don't know about**. Our focus has been illuminating what they don't currently know, so teams can stop pervasive threats that may otherwise blindside them.

It's our belief that enterprises cannot truly reduce their risk of attacks that leverage stolen identity data unless they understand and act on the user exposure holistically. A user's exposure across their personal and professional digital lives matters to the business, whether they're an employee of the company, a consumer of their products, a vendor/partner supplying goods and services – or a criminal.

SpyCloud is best-suited to illuminate the real risks, visualize them, and help customers act on them fast – and with confident precision.

Our focus has led us to hone our craft in three interconnected areas that we consider core to identity threat protection:

REAL-TIME, RECAPTURED DARKNET EXPOSURE DATA

It starts with the world's largest, continuously updated repository of ***breach, malware- exfiltrated and successfully phished data,*** with more than 200 data types, clean and curated, from passwords and cookies to financial information and sensitive PII.

COMPREHENSIVE AND ACTIONABLE IDENTITY ANALYTICS

Dynamic identity correlation synthesizes data from diverse sources to enable full understanding and visualization of the extent of stolen data tied to your employees, consumers, and vendors – ***the scope of exposures that make your business a target.***

AUTOMATED REMEDIATION WITHIN YOUR EXISTING TOOLS

With rapid remediation in your IdP, SIEM, SOAR, TIP, or EDR ***in as little as 15 minutes*** from discovery of the exposure – you can comprehensively reduce risk without more resources or more sleepless nights.

BENEFITS ACROSS A VARIETY OF USE CASES

We've evolved our offerings at SpyCloud to incorporate a more holistic approach to solving for identity threats, setting a new standard for security and fraud prevention teams charged with preventing cybercrimes. Below, we outline the specific impacts our customers are experiencing with a broad understanding and automated remediation of darknet exposures.

PREVENT ACCOUNT TAKEOVER

Enterprises with a traditional account takeover prevention solution – typically, a monitoring service for alerting on compromised credentials – are limited by only being able to react to exposures stemming from the corporate identity specifically; for example, resetting a password when a user's current, in-use password is leaked in a third-party breach. The key abilities introduced by holistic identity threat protection are:

- Forcing passwords changes when exposed passwords tied to a user's past or present personal and work accounts have been reused or recycled
- Preventing personal password reuse in the workplace when exposures tied to personal accounts are correlated to a corporate username/email with no darknet exposures
- Terminating compromised web sessions tied to stolen cookies exfiltrated from a managed or unmanaged malware-infected device

SpyCloud's holistic identity threat protection prevents – for the first time ever – password reuse and recycling of passwords that are in any way correlated to the user's holistic identity. This is a massive win for security and identity teams, as you can now protect the business from exposures well beyond the current visibility you may have today.

FEATURED PRODUCT:

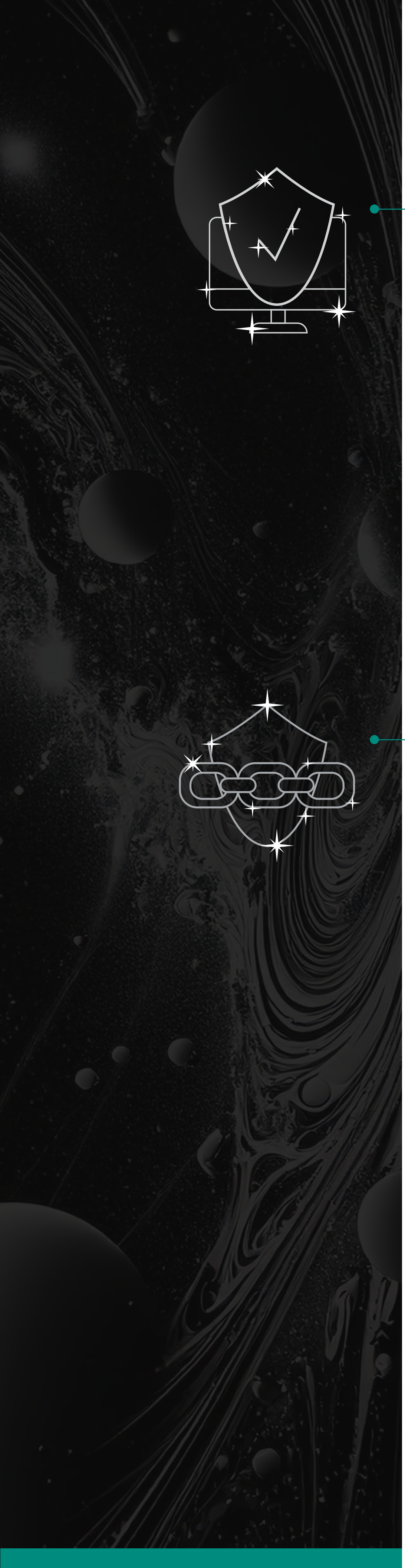
SpyCloud Active Directory Guardian

Automatically identify and take appropriate action on exposed passwords that would otherwise be hidden behind an employee's personal identity – remediating 7x more exposures than exact matching allows.

CONTINUOUS ZERO TRUST

Traditional Zero Trust implementations leave gaps when they only check the validity of users and devices upon first access to the network. A holistic identity approach takes your Zero Trust strategy to an entirely new level – continuously feeding your policy engine with advanced telemetry on employee identities that have been exposed outside of the strictly corporate viewpoint.

Identity threat protection from SpyCloud enables continuous identity monitoring, resulting in always-on authentication and no blindspots. Your team gains expanded visibility into malware-infected employees and other identity exposures, and can take quick action with the appropriate policies to automate remediation.



PREVENT RANSOMWARE ATTACKS

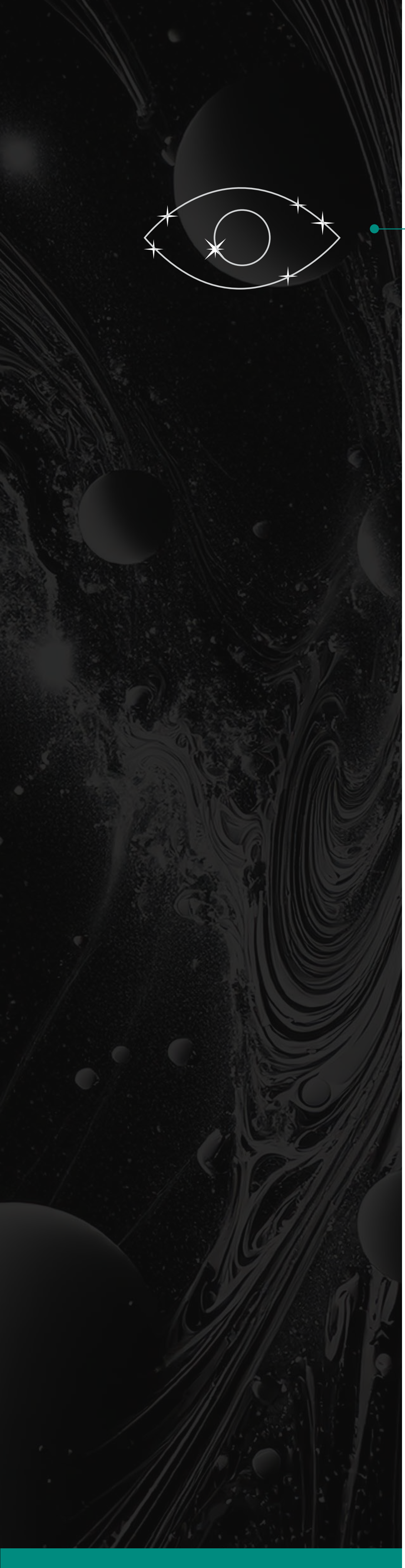
Recent research shows security teams share **universal concern** about ransomware risk from darknet exposures, including infostealer malware, with security teams investing in improved visibility and remediation of malware-exfiltrated credentials and cookies. Given account takeover's prevalence as a precursor to ransomware, it makes sense – whether the criminal leverages stolen credentials or authentication cookies to gain a foothold within the organization. But stolen user data provides the pretext for another way in, via social engineering. All entry points must be accounted for in a robust cybersecurity program.

Holistic identity threat protection delivers an expanded view of identity exposures that light up a path to ransomware prevention – giving defenders the power to thwart the relationship between account takeover and ransomware once and for all.

MITIGATE SUPPLY CHAIN THREATS

Traditional supply chain risk management solutions focus on high-level risks, instead of actionable threats that an organization's vendors might face. Focusing on vendor risk helps in classifying the overarching risk to the enterprise, which can help to build a strong profile for compliance purposes – but without additional threat information, there are very few options for mitigating that risk.

Understanding threats to your suppliers through the exposures of their employees' holistic identities is just as important as understanding the risks facing your own employees. With so many vendors being used as the point-of-entry in prominent attacks, it is critical for every enterprise to understand where significant threats exist within their supply chain to prioritize increased protective mechanisms. Additionally, early notification of significant malware, phishing, and breach threats provided to the affected vendors helps them avoid follow-on, targeted cyberattacks.



DARK WEB MONITORING

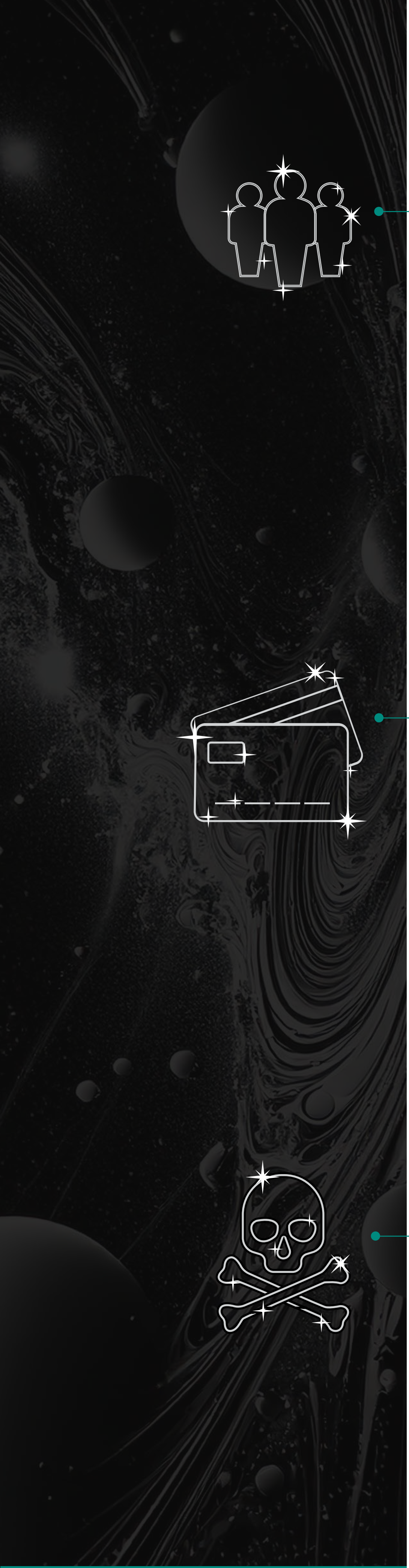
Many threat intelligence solutions exist to provide dark web monitoring, alerting enterprises or consumers to events that have been observed in the criminal underground that could somehow impact them. The majority of such solutions focus on “dark web chatter,” which represents communication sessions between criminals and collect credentials from the “surface” of the darknet, such as pastebins and publicly available sites, where the data is typically old and has already been monetized by criminals. While these solutions can provide valuable context, the information provided can be very challenging to connect to specific threats that can be automatically remediated.

Superior dark web monitoring solutions focus less on context and more on key elements that represent true threats facing the enterprise’s employees or consumers being monitored. In order to truly understand how an individual might be targeted, the dark web monitoring service must look at data the same way criminals do – and at each involved individual holistically.

Effective dark web monitoring requires a holistic identity perspective. Monitoring events connected to an employee’s or consumer’s holistic identity allows for a broad view of the user being analyzed. Acting on recaptured data, such as credential, financial, and PII data that can be connected to the user across their many online personas, ensures that none of this critical information can be used in ATO, BEC, fraud, social engineering, or a variety of follow-on attacks. Remediation actions can range from:

- Terminating active sessions associated with users connected to malware-infected devices
- Clearing stored credit card data
- Requiring step-up authentication or password resets when any exposed password connected to a user’s identity is being actively used
- Preventing the selection of passwords that are in any way connected to the user’s holistic identity exposures
- Monitoring accounts for suspicious behavior

Identity monitoring solution providers can also **enhance their offerings** with a holistic identity perspective, providing even more value to users.



KNOW YOUR CUSTOMER (KYC)

Understanding the comprehensive identity exposure of consumers has profound effects on Know Your Customer (KYC) processes. Financial institutions need more robust identity verification mechanisms to detect potentially fraudulent new accounts and credit applications, as well as unusual combinations of personal data from stolen identities. Frankly, the correlation of an individual's PII exposures across their dozens of breaches and data leaks is now a necessity for combating the most complex identity crimes, from "true name" fraud to synthetic identities.

Incorporating a holistic identity POV into KYC protocols strengthens the ability to verify customer identities, reducing the risk of fraud and ensuring compliance with regulatory standards. A broader view of a consumer's identity exposures also allows for more accurate risk profiling, leading to tailored due diligence measures.

FRAUD PREVENTION

In order to prevent consumer fraud, it is critical to understand whether the user attached to a particular account has information about them being traded on the darknet. Having access to the account details provides criminals with a variety of tools that can be used for account takeover and fraudulent transactions.

However, solutions that include a holistic identity perspective provide fraud prevention teams an extended view of a user's risk and can provide dramatically greater levels of protection for the organization. Knowing whether a user has other email addresses and usernames, credit card data, and PII exposed across their many other online accounts enhances fraud decisioning – enabling more comprehensive and faster payment fraud detection, and the implementation of proactive measures like card replacement and account monitoring.

THREAT ACTOR ATTRIBUTION

A holistic identity lens has a major impact on attribution analysis – investigating the criminals behind attacks and tying their crimes to specific individuals or groups. Unknowns can become known with the click of a button and alternate identities can be unmasked with little effort – enabling you to tie activities to these identities and boost your investigations and root-cause analysis by multitudes.

INCIDENT RESPONSE

During and after an active incident, IR analysts need the ability to rapidly understand the identities that can be connected to any specific selector associated with the attack. Correlating those selectors to any other user information, PII, system data, or access patterns can speed the discovery of how the actor gained initial access, and helps analysts understand the blast-radius of the attack – both critical steps in the Incident Response process.

Using SpyCloud's automated holistic identity analysis, the IR analyst can rapidly expand the scope of the search beyond the initial email or username to include a wide range of account types. In IR investigations supported by SpyCloud Investigations with integrated identity analytics, analysts have reported **400% improvement in investigation times**, and less senior analysts making discoveries that previously required very senior analyst expertise. In the world of IR, shaving hours off the clock while discovering more about the attack can dramatically limit the damage and the aftermath.

DETECT & MITIGATE INSIDER THREATS

Intentional, malicious insiders plague security teams everywhere. But a better understanding of a user's holistic identity can aid security teams in their discovery and investigation of insider threats, especially when bolstered with insights like the user's associations with suspicious or illicit online forums.

Through the analysis of a user's holistic identity, you can more easily identify malicious insiders that may have online identities linked to darknet forums where they could be selling corporate IP – and do so without them having to make a critical mistake to get caught. Without automated analysis of the holistic identity, it would take advanced investigators and analysts hours to perform this type of correlation, if at all. Holistic identity threat protection saves teams time and more effectively mitigates insider threats before they cause harm to your organization.

FEATURED PRODUCT:

SpyCloud Investigations

Discover and act on threats with automated identity analytics that illuminate the scope of digital identities and accelerate successful outcomes of complex investigations from days or hours to minutes.

HOLISTIC IDENTITY THREAT PROTECTION CHANGES THE GAME.

Holistic identity as a new and critical component of identity security use cases is a complete game changer. Traditional solutions for identity management, threat intelligence, incident response, and identity security rely heavily on the specific user account managed by your enterprise and leave the door open to unseen risk. When you respond to the holistic identity, you can leverage the breadth of data that criminals are leveraging – ensuring it cannot be used against you.

This change in identity threat protection not only allows you to provide automated protection from identity threats, but also provides you with revolutionary tools to investigate and respond to all manner of cyberattacks. Understanding the broad holistic identity can dramatically speed your incident response analysis and significantly improve the total time required to develop attribution.

Simply put, incorporating a holistic identity lens into the way your enterprise manages these key use cases helps you realize a level of identity protection that has not existed before. With this shift, you can act on the broad scope of information that was previously only understood by the criminals, stopping costly, damaging attacks before criminals have a chance to act.

With SpyCloud, you can close dangerous open doors and drastically improve the protection of your enterprise and consumers.

ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to disrupt cybercrime. Its automated identity threat protection solutions leverage advanced analytics to proactively prevent ransomware and account takeover, safeguard employee and consumer accounts, and accelerate cybercrime investigations. SpyCloud's data from breaches, malware-infected devices, and successful phishes also powers many popular dark web monitoring and identity theft protection offerings. Customers include more than half of the Fortune 10, along with hundreds of global enterprises, mid-sized companies, and government agencies worldwide. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to protect businesses and consumers from the stolen identity data criminals are using to target them now.

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

SPYCLOUD.COM