Constella

2025 Identity Breach Report

Mapping the Evolving Identity Attack Surface

2025 | Annual Report

Constella

Table of Contents

Foreword

Identities have become the ultimate gateway to organizational and personal assets. The growth and expansion of the identity attack surface has accelerated dramatically, driven by relentless innovation in technology, adversarial tactics, and the growing industrialization of digital risk. In the 2025 Identity Breach Report, Constella Intelligence provides a critical and timely exploration of this growth and transformation, mapping out how identity related risks have evolved from isolated incidents into sophisticated, scalable, and highly automated operations.

As this new era of hyper-connected environments and relentless digital acceleration enters our daily lives, understanding the dynamics of identity risks is paramount. Nefarious actors have industrialized their methods, leveraging automation, AI-driven tools, and robust data-driven strategies. All of these enable them to execute attacks at unprecedented scale and speed, while achieving concerning levels of precision. This evolution demands an equivalent transformation in how organizations perceive and manage identity risks, shifting from reactive, event-driven responses to proactive, intelligence-driven defense strategies.

At the core of this transformation lies the enriching and powerful notion of Identity Risk Intelligence. Constella Intelligence's latest insights highlight this essential concept, underscoring the pressing need for continuous and context-rich monitoring, predictive intelligence, and adaptive defenses that anticipate threats before they materialize. Organizations must now harness Identity Risk Intelligence that is backed with a large data set of high fidelity. This combination will facilitate and empower real-time analytics and adaptive authentication processes to safeguard environments at varying levels of operations.

The 2025 report serves not just as an analysis but as a strategic guide to navigating this complex and rapidly industrializing identity-centric threat landscape. It emphasizes the importance of proactive vigilance, strategic resilience, and informed leadership in combating identity-driven threats.

I encourage security leaders, decision-makers, and all stakeholders invested in digital security to carefully study this report. Equip yourself with the insights needed to secure your organization against the rapidly evolving identity threat landscape of today, and tomorrow.

Andres Andreu
COO & CISO, Constella Intelligence

About Constella's Identity Breach Report

Constella's threat intelligence team continually collects identity records from data breaches and leakages across various sources, including open, surface, social, deep, and dark web. This comprehensive data tracking focuses on identifying breaches related to companies and the specific Personally Identifiable Information (PII) exposed, which poses risks to organizations, their employees and customers. With over 230 billion identity records and more than 1.1 trillion curated identity assets, Constella provides unparalleled insights to help manage these risks.

The rapid advancement of artificial intelligence (AI) and the vast growth of digital identities have significantly reshaped the cybersecurity landscape. Sophisticated AI tools and the proliferation of digital data are leading to more targeted and complex cyber threats.

This report aims to highlight these emerging trends and offer actionable insights to assist organizations in strengthening their cybersecurity measures. By understanding these evolving threats, organizations can better anticipate risks and implement effective strategies to safeguard their data and systems in an increasingly intricate digital environment.

Harness the Power of the World's Largest Identity Risk Data Lake.

>1.1T
Identity Assets

Powered by our data lake of greater than one trillion curated and verified assets

230B+
Identity Records

Our data spans

125
countries

53
& languages

15+
years of historical data

Executive Summary

In 2024, identity moved further into the crosshairs of cybercriminal operations. From mass-scale infostealer infections to the recycling of decade-old credentials, attackers are industrializing identity compromise with unprecedented efficiency and reach. This year's data exposes a machine-scale identity threat economy, where automation and near-zero cost tactics turn identities into the enterprise's most targeted assets.

Constella Intelligence's unique visibility across breach data, infostealer malware, and identity-centric exposures provides a singular view into the evolving tactics, techniques, and ecosystems driving today's cyber threats. This report distills insights from over 219K breach events, 107.1 billion exposed records, and 30 million infected devices to map the contours of the new identity attack surface – and the industrial operations behind it.

For security leaders, the implications are clear: credentials are currency, PII is fuel, and executive identities are high-value targets. Protection strategies must evolve beyond perimeter defense to proactively detect and mitigate identity exposures – across employees, vendors, and VIPs – before they're weaponized.

> "Valid account credentials and exploitation of public-facing applications each accounted for 30% of initial access vectors in 2024, continuing the trend of attackers logging in rather than hacking in."
>
> – IBM X-Force 2025

Key Data Insights

1

IDENTITY IS THE NEW ATTACK SURFACE

More and more attackers are logging in with stolen credentials rather than breaching through other means – and stolen credentials are easily bought and sold on the dark web.

2

INFOSTEALERS NOW MASS-HARVEST IDENTITIES AT SCALE

Hackers now capture live session cookies, credentials, and browsing behavior and rapidly weaponize that data for Account Takeover (ATO), fraud, and lateral enterprise compromise.

3

IDENTITY BREACH IMPACT GOES FAR BEYOND JUST THE IT TEAM

The level of identity leakage drives synthetic identity fraud, phishing precision, and regulatory exposure, raising the enterprise breach cost beyond IT to legal, compliance, HR, and brand teams.

4

CYBERCRIMINALS RECYCLE BREACHED DATA INDEFINITELY

This means your exposure never expires – even if a user resets their password, the same email, name, and partial PII often remain viable, often due to lack of rigor around identity security.

5 CXO DIGITAL EXPOSURE AND CREDENTIAL LEAKS ARE INCREASING

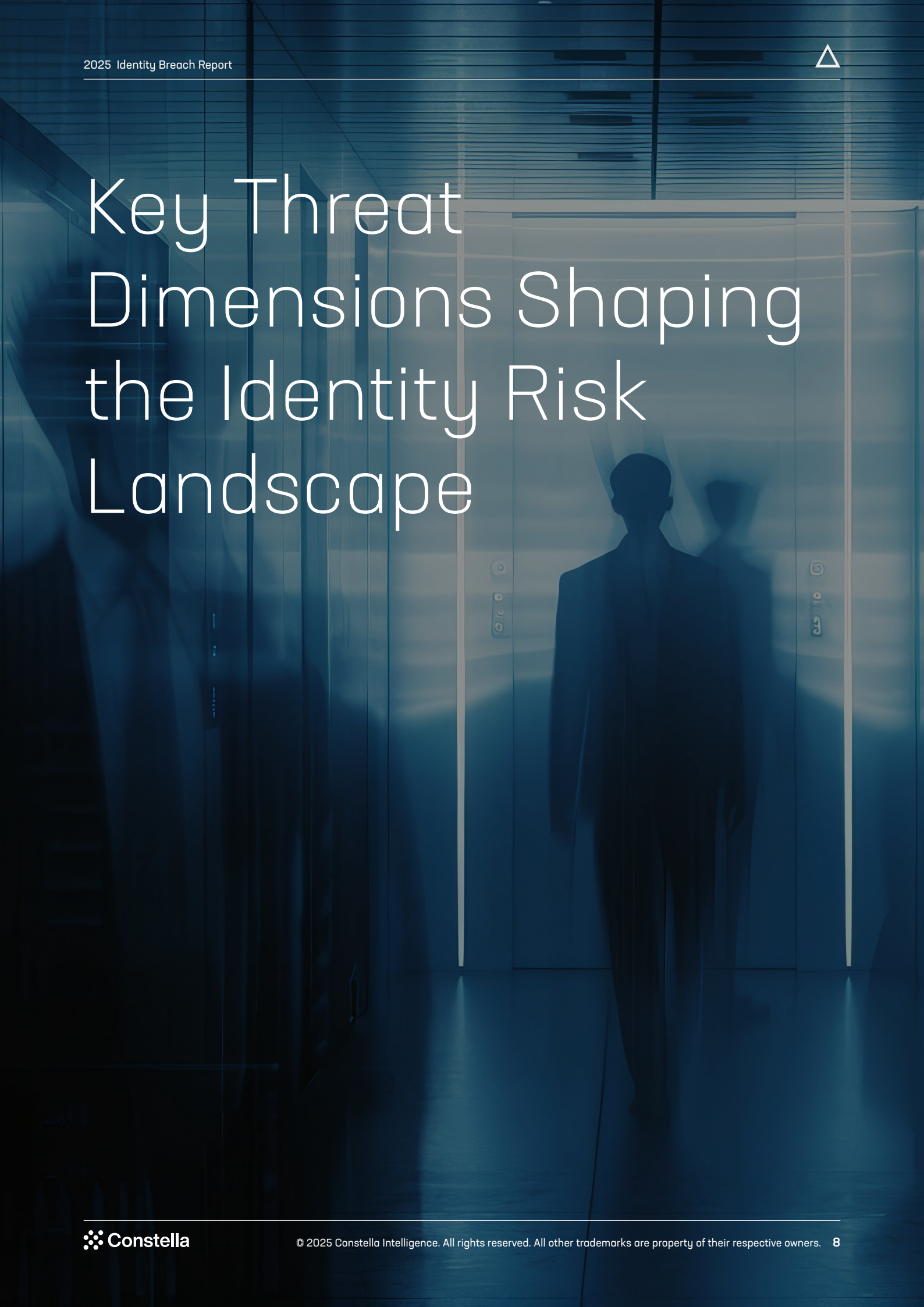
Leaked executive identities give attackers privileged access, influence, and high-value targets for fraud or social engineering. The exposure of a CxO is no longer rare – it's recurring, and too often invisible until exploited.

6 SUPPLY CHAIN IDENTITY RISKS AMPLIFIES BREACH IMPACT

Identity breaches are now often multi-hop events, with compromises in one organization leading to intrusions in its partners or clients. Attackers target the weakest links – smaller vendors, contractors, or cloud platforms – to leapfrog into high-value targets.

7 AGENTIC AI: THE NEXT FRONTIER OF THREATS AND DEFENSE

The rapid rise of generative AI is a double-edged sword. On one side, defenders gain powerful new tools for threat detection and analysis. On the other hand, criminals are experimenting with "agentic AI" – autonomous AI systems that can act on malicious intent at scale and with precision.



Key Threat Dimensions Shaping the Identity Risk Landscape

Identity is the New Attack Surface

In 2024, digital identities – usernames, credentials, and personal data – continued to eclipse infrastructure as the most targeted enterprise assets. With over 1 billion identity records exposed via breaches and infostealers, attackers increasingly log in instead of breaking in.

Credential harvesting emerged prominently, identified by IBM X-Force as the primary impact in **30% of incident response cases***. Due to their relative ease and scalability, attackers prioritize valid credentials over more complex, malware-driven tactics.

Constella's threat intelligence operations underscore this trend, having hunted down over 219K breaches and ingested approximately 11.8B records in 2024 alone. Notably, 6.4B of these records included email addresses, with over 4.3B unique emails newly indexed – a startling 58% increase year-over-year. Password exposure also reached alarming levels, appearing in over 2.5B records, either in plaintext or hashed formats, highlighting the extensive nature of credential compromise.

*IBM X-Force 2025 Threat Intelligence Index: https://www.ibm.com/reports/threat-intelligence

TREND ALERT

Juxtaposition Between Number and Scale of Incidents

According to the Identity Theft Resource Center, the number of reported breaches in 2024 remained flat compared to 2023.*[1] However, Constella's data reveals an increase. This discrepancy may point to a significant volume of unreported or unofficial breaches, as well as a rise in resurfaced incidents – previous breaches that are re-leaked, recompiled, or re-sold under new distributions.

Unlike traditional breach trackers, Constella monitors a wide array of sources across the surface, deep, and dark web, enabling the detection of breach data that may never be formally disclosed. This highlights the growing need for continuous monitoring, deduplication, and curation of breach data to distinguish truly new exposures from recycled or re-emerging ones. Without this level of visibility, organizations risk underestimating their exposure in the identity threat landscape.

Today's attackers leverage compromised digital identities as their primary entry points, bypassing traditional defenses that focus solely on endpoints and network firewalls. Comprehensive protection now requires vigilant monitoring of both corporate and personal digital identities to proactively mitigate emerging threats targeting executives and other high-risk individuals.

> "Fewer breaches, but far greater damage. It's no longer about how many breaches occur, but how extensive their reach is."
>
> - Identity Theft Resource Center

*[1] www.idtheftcenter.org: 2024 Data Breach Report *[2] axios.com

Recommendations

By focusing on identities, organizations can start to bend the breach trend curve back in their favor. The goal is to make using stolen credentials as difficult as possible for attackers, and to catch them quickly when they try – mitigating the sprawling, multi-million-record disasters that defined 2024. Tactics orgs can implement:

1

ADOPT AN IDENTITY-CENTRIC SECURITY STRATEGY

Treat compromised credentials and PII as the top risk. Implement solutions for continuous identity threat monitoring – for example, services that alert you if your employees' emails or passwords surface in a breach dataset.

2

SHRINK THE BLAST RADIUS

Since breaches are hitting more records per incident, limit what any single account or system can access. Follow least privilege principles – for example, an accounting employee's account should not have access to millions of customer records if not necessary.

3

IMPROVE BREACH RESPONSE & NOTIFICATIONS

Update/create an incident response plan that specifically covers identity-related breaches. This includes playbooks for rapidly analyzing which accounts may have been compromised (through logs, comprehensive breach intel, etc.), and automating forced password resets or access revocation.

4

INVEST IN ZERO TRUST ARCHITECTURE

Double down on Zero Trust principles, which "verify continuously" rather than trusting a one-time login. Implement continuous anomalous behavior detection – for instance, if a valid user suddenly accesses large data sets at 3 a.m., treat it as a potential breach and investigate.

Summary: To counter the rise in large-scale breaches, organizations must adopt identity-focused defenses. This includes real-time credential monitoring, limiting access scope, strengthening breach response, and applying Zero Trust principles. These tactics reduce exposure, contain damage, and speed up detection. In a landscape of sprawling threats, identity is the frontline.

02 Infostealers Now Mass-Harvest Identities at Scale

Constella's telemetry observed over 30 million infostealer device logs circulating on dark web marketplaces in the past year. These logs are essentially data dumps from infected machines, often containing a wealth of information: saved logins and passwords from browsers, cookies that keep sessions authenticated, autofill credit card details, system information, and sometimes screenshots or browser histories. Each log provides a multiplexed attack vector, containing credentials, session cookies, wallet files, and application tokens exploitable within minutes.

External reports mirror this surge. IBM noted an **84% year-over-year increase in phishing campaigns that deliver infostealer malware***[1]. In other words, email threats shifted heavily toward dropping these stealers to gather credentials.

Why are infostealers so popular? In short, ROI.

They are relatively easy to deploy (many operate on a malware-as-a-service model where criminals rent access), they quickly return valuable data (passwords to bank, email, VPN accounts, etc.), and they carry less risk and noise than overt attacks. A ransomware attack immediately announces itself to the victim; an infostealer infection might never be noticed at all.

From a single infostealer-infected PC, a hacker can gain footholds into multiple accounts and systems.

One of the largest ongoing data leaks in history, in fact, is not a single breach but the aggregate result of infostealers. Constella's researchers have tracked infostealer infections impacting machines in virtually every industry. Notably, when **50 recently breached companies were studied, 78% of them had corporate credentials found in infostealer logs** in the six-month window around their breach*[2]. This suggests a strong correlation: either infostealers contributed to those breaches (stealing an employee's password that was later used by attackers) or attackers planted infostealers during or after the breach to gather more data. Often, both are true.

This growing threat is exemplified by the rise of advanced malware families. Among the most common seen in 2024 were LummaC2, Redline, and Vidar. LummaC2 infections doubled in the third quarter, driven by its ability to rapidly exfiltrate stolen data and obscure attacker activity using SOCKS proxying. These features make it easier for cybercriminals to harvest credentials and session cookies without detection – highlighting just how stealthy and scalable modern infostealers have become. It's essential that this risk is clearly communicated to both technical and non-technical stakeholders as it poses a widespread and largely invisible threat to organizations of all sizes.

[1] siliconangle.com / [2] channele2e.com

TREND ALERT

Corporate Risk: Infostealers as Pre-Breach Indicators

Infostealer infections are no longer just about stolen credentials – they're often the starting point for full-scale cyberattacks. When caught early, even on a personal device, an infostealer infection can serve as a crucial red flag. With rapid response, security teams may be able to prevent broader compromise. But in many organizations, visibility remains limited. Personal devices are rarely monitored, and corporate endpoints lacking EDR (Endpoint Detection & Response) are especially vulnerable, particularly when the malware is new and evades traditional antivirus detection.

According to CrowdStrike's 2024 Global Threat Report,* over 30% of ransomware incidents began with access gained through infostealer infections. This underscores the dual-threat nature of infostealers: they not only harvest credentials but also serve as initial access vectors for high-impact, enterprise-wide disruptions. What begins as a silent infection can escalate into a catastrophic breach if left unaddressed.

> Infostealer infections are often the breach before the breach.

Infostealers are reshaping insider threat assumptions. Previously, a cluster of employee credentials appearing for sale might raise flags about insider activity. Today, malware should be the default assumption. Are these employees infected? It's often not a matter of negligence or intent, but undetected cyber compromise.

And they're targeting more than just passwords. Modern stealers are evolving to capture cryptocurrency wallets, authentication token files, and even documents. As enterprises move toward token-based and passwordless authentication, attackers are adapting. Any data that enables identity impersonation, or lateral movement, will be in their sights.

*Crowdstrike 2025 Global Threat Report

Recommendations

Defending against infostealers requires both technical and human countermeasures. Here's what leadership should ensure is happening:

1

ELEVATE USER AWARENESS AND DIGITAL HYGIENE

Employees (and executives) should be regularly trained about the dangers of downloading pirated software, cracked games, or clicking unknown links – even on personal devices. Infostealers often enter via consumer-facing lures. Security awareness should go beyond phishing and cover tactics like fake browser updates, misleading ads, and rogue plugins – common delivery methods for infostealers.

2

MONITOR FOR INFOSTEALER EXPOSURE

Use threat intelligence feeds (like Constella's) to detect if your organization's credentials appear in underground logs. When found, immediately reset affected credentials and investigate for signs of compromise – this early warning can surface issues before attackers act. Integrate exposure alerts into your incident response workflow, and track exposure trends over time to identify systemic weaknesses.

3

ISOLATE ENDPOINTS FOR HIGH-RISK USE

For privileged users or those handling very sensitive data, consider dedicating separate devices or virtual environments that are locked down. For instance, an admin might have a special locked-down laptop for server access that doesn't allow web browsing or installs. This mitigates infostealers getting in.

4

CONDUCT RAPID INCIDENT RESPONSE DRILLS

Operate under the assumption that an infostealer will eventually compromise an employee. Run internal drills to test your response – for example, simulate a scenario where the security team is alerted that an employee's password has been found in a stealer log. Walk through each step of the response: disable the affected account, scan the employee's devices, confirm malware removal, and assess whether the compromised credential was reused across other systems.

Summary: By treating infostealer infections as the serious breaches-in-waiting that they are, organizations can significantly reduce the risk of a silent credential compromise turning into a full-blown disaster. In the broader scope of identity breaches, curbing infostealers is like cutting off the adversary's supply lines.

Identity Breach Impact Goes far Beyond Just the IT Team

In 2024, personally identifiable information (PII) exposure reached unprecedented levels, appearing in 99.33% of breaches – even higher than 96.6% last year. Nearly every breach involved sensitive data beyond basic credentials, encompassing full names, addresses, phone numbers, birthdates, and even Social Security numbers (SSNs) and credit card details. Specifically, breaches exposed over 2B records with full names, 4.2B phone numbers, and 2.9B addresses and cities. Further, sensitive information like birthdates (1.05B), approximately 519M SSNs, and approximately 225M credit card numbers were compromised.

The pervasive exposure of PII redefines the breach impact narrative, significantly widening the blast radius for affected organizations. Enterprises now face escalated risks extending beyond IT security into:

- Legal compliance
- Regulatory penalties
- Fraud prevention
- Substantial brand reputational damage

Boards and executives must recognize that identity theft and synthetic identity fraud, driven by comprehensive identity data leakage, represent critical vulnerabilities. Targeted social engineering attacks and sophisticated deepfake threats leverage the smallest toehold of identity exposure. This risk demands a strategic realignment from traditional breach responses toward comprehensive digital risk protection and identity monitoring strategies. Heightened financial and reputational risks underscore the importance for CISOs, CIOs, and executive leaders to adopt robust protective measures across their entire digital footprint.

TREND ALERT

The Commoditization of Personal Data

Personal data has become so abundant that its black-market value has plummeted – yet its threat impact has only grown. Criminals now buy or even download for free massive datasets of PII, often packaged as "fullz" (full identity kits), which are often available for less than $5. With these kits, attackers can easily synthesize fake identities or impersonate real ones to carry out sophisticated scams, including tax fraud, medical fraud, and fraudulent account onboarding.

Constella's intelligence team has tracked the rise of composite identity records, where threat actors merge multiple breach sources to deepen insight. For example, one breach may expose a name and email, another adds a phone number, and a third leaks a cracked password. When aggregated, these details allow for highly targeted attacks like spear phishing or social engineering.

Threat actors increasingly use techniques – maintaining searchable databases indexed by email or phone – to instantly surface everything known about a target across breaches. These are effectively black-market CRM systems powered by recycled PII.

This commoditized data fuels fraud tactics such as new account creation, credential stuffing, and identity-based phishing. Massive "combo lists," like the 3.2 billion-record COMB breach, make it easy for attackers to connect fragmented data points, often aided by automation or AI.

> The oversupply of personal data has driven down its black-market price – but dramatically increased its threat potential.

Recommendations

To mitigate the risks associated with massive PII exposure, leaders should drive a multi-pronged response:

1

LIMIT DATA COLLECTION AND RETENTION

Re-evaluate what personal data you collect and store. Avoid holding unnecessary PII. For required data, use anonymization or tokenization, and apply strict retention policies – delete data no longer needed for business or legal reasons.

Limiting the volume of stored data not only reduces exposure risk, but also simplifies compliance with evolving privacy regulations.

2

PROVIDE IDENTITY THEFT PROTECTION

Offer identity protection services post-breach – and ideally, before. Extend monitoring to employees, high-risk customers, and especially executives, whose continuous protection helps catch misuse of personal data early. These services act as an early detection layer, enabling faster reaction to fraud and minimizing long-term reputational damage.

3

IMPROVE INCIDENT RESPONSE FOR PII BREACHES

Build detailed PII-specific breach plans with clear steps for triage, investigation, compliance, and customer comms. Run simulations to ensure teams can respond quickly and under pressure. A rehearsed, identity-aware response limits confusion, ensures transparency, and helps meet regulatory deadlines.

4

LEVERAGE IDENTITY INTELLIGENCE

Use services like Constella to monitor dark web leaks for your domains and customer patterns. Early alerts turn exposed PII into actionable insights – triggering password resets, fraud warnings, or other defensive steps. Linking identity intelligence with breach response empowers teams to act before data abuse escalates into a full-blown incident.

Summary: By combining prudent data governance with proactive security and response, organizations can navigate this era of ubiquitous personal data leakage and protect both themselves and their stakeholders from the worst outcomes.

04 Cybercriminals Recycle Breached Data Indefinitely

A significant portion of breach activity in 2024 revolved around the recycling of previously exposed identity data. Constella's analysis revealed that **nearly 60% of the breaches ingested consisted of credential compilations rather than fresh compromises, marking a notable increase from 43% in 2023.** These "combo lists" repurpose records from historical breaches, recycling them into new, highly effective credential-stuffing sets. In fact, only 7.4% of breaches in Constella's massive data lake represented truly unique breach or leak events.

The perpetual circulation of identity data underscores a critical industry reality: **breaches effectively never end**. Cybercriminals continuously exploit and re-exploit existing leaks, sustaining persistent threats against individuals and organizations alike. Over 4.2B unique email addresses were identified in Constella's monitoring activities, demonstrating the extensive and enduring nature of recycled identity threats.

For CISOs, CIOs, and executive leaders, **this persistent recycling of breached identity data mandates a shift toward continuous exposure monitoring and proactive threat intelligence**. Organizations must extend their protective strategies beyond reactive password resets, recognizing that emails, names, and partial personal identifiers remain perpetually vulnerable to impersonation, phishing, and targeted social engineering. Educating users on the heightened risks associated with credential reuse is now an essential component of comprehensive cybersecurity defense.

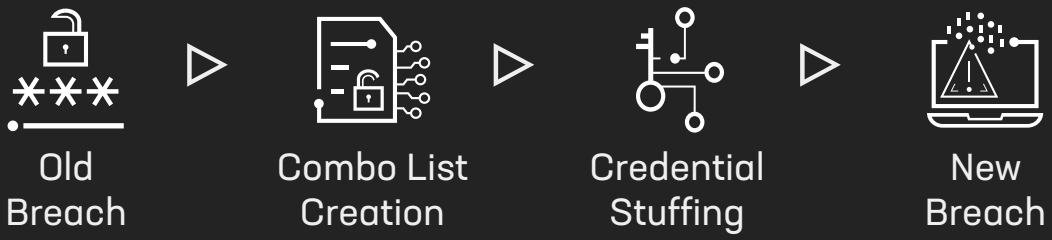
TREND ALERT

Synthetic Identities and Stitching Data Together

Last year's report* introduced synthetic identities as an emerging trend. This kind of recycling is where criminals construct a new identity (one that doesn't correspond to a real person) using pieces of real PII. For instance, they might take a real social security number of someone who doesn't use credit (like a minor or deceased individual, obtained from leaks), combine it with a fake name and a real address from another breach, and create a "person" that passes employee background and new customer credit checks. They then open bank accounts, credit lines, etc. in that fake identity's name – often riding under the radar until they max out loans and vanish. Synthetic identities often pull from breached data to appear legitimate (e.g., using a real SSN ensures the credit bureaus have a record).

60% of breaches are based on reused identity data

The availability of data for sale in underground markets makes this easier than ever. Constella's threat experts regularly see listings like "500 fullz of US customers – includes SSN, DOB, full name, address, email," which clearly are compiled from breaches or insider theft. Those "fullz" feed the synthetic ID mills. In 2025, financial institutions are bracing for a wave of such fraud, which is hard to detect because no single piece triggers alarms (the SSN is valid, the person just has no prior history – which can look like a young adult or a new immigrant).



*2024 identity breach report: https://constella.ai/2024-identity-breach-report

Recommendations

Given the evergreen nature of breach data, organizations must assume that some of their credentials and personal data are already exposed. Here's how to counter the threats of recycled identities:

1

MANDATE STRONG, UNIQUE PASSWORDS + PASSWORD MANAGERS

The single best defense against credential reuse attacks is to ensure your users (employees and customers) aren't reusing passwords. Enforce strong password policies and consider providing password manager tools to employees so they can easily manage unique passwords.

2

MONITOR UNUSUAL ACCESS PATTERNS

Watch for spikes in failed logins – common signs of credential stuffing – and use anomaly detection to block abusive IPs. Also monitor for successful logins from unusual devices or locations, which may indicate compromised credentials were used.

3

CONDUCT SYNTHETIC IDENTITY CHECKS

Strengthen employee-onboarding and account-opening processes by going beyond static PII like SSNs. Use document verification, device intelligence, and services that flag anomalies or synthetic identities. Join consortium databases to detect and prevent fraudulent identity creation attempts in real time.

4

SHARE INTEL CROSS-ORGANIZATIONALLY

Join threat-sharing groups (ISAOs, ISACs) to identify credential-based attack patterns. Shared intelligence helps surface coordinated credential stuffing campaigns early – especially when attackers reuse the same stolen credentials across multiple companies or sectors simultaneously.

Summary: Combating recycled identity threats is about not giving attackers an easy win with old data. It requires both technology (detection, MFA, etc.) and user behavior changes. The more we can render breached data obsolete (through non-reuse and good security hygiene), the less value it holds for attackers over time.

CXO Digital Exposure and Credential Leaks are Increasing

The executive threat surface quietly and significantly expanded this past year, as Constella observed a notable surge in breaches and infostealer logs that specifically contained data from executives and other high-privilege users. Threat actors target individuals who hold strategic, financial, or operational influence because they recognize them as valuable leverage points for attacks and exploitation.

Constella's 2024 data highlights the scale of this emerging threat: executive and employee identities featured prominently in infostealer logs across global regions, including over 417K employees in North America and approximately 15K employees in Asia. Furthermore, executive domains – corporate email addresses linked to high-ranking individuals – regularly appeared in breach compilations and malware logs, underscoring the repeated exposure of these strategically valuable identities.

> Threat actors target individuals who hold strategy, financial, or operational influence.

The visibility and prevalence of executive-level identity leaks empower attackers with privileged access and leverage for highly targeted fraud and sophisticated social engineering attacks. CXO identity exposure is now frequent and persistent, often remaining undetected until leveraged in an exploitative attack. Organizations must proactively extend their cybersecurity framework to safeguard executive identities, mitigating risks before exploitation occurs. The net effect is a bullseye on executives. A 2024 survey by GetApp found 72% of cybersecurity pros observed senior executives being targeted recently, and 54% of U.S. companies had an identity fraud incident affecting an executive*[1]. Moreover, an increasingly common element is AI-driven impersonation – 27% of those attacks on execs involved deepfakes*[2].

*[1] businesswire.com / *[2] businesswire.com

TREND ALERT

Zooming in on Deepfakes

While we touched on deepfakes in last year's report* and above, there has been a noticeable uptick in these insidious efforts. With AI, hackers can now create deepfake videos using just minutes of publicly available executive footage and voice samples. These AI-generated impersonations are being used to deceive employees, investors, and partners in high-stakes phishing and wire fraud schemes.

The result? A growing executive threat surface that looks and sounds legit.

How are deepfakes are being created and leveraged?

- **Multi-Channel Convergence:** Attackers combine email, phone calls with deepfake voices, and even video deepfakes to build trust. This layered approach increases credibility and pressure, making the scam far more convincing than a single-channel phishing attempt.
- **Quality and Accessibility:** Deepfakes are getting more realistic, and easier to create. With just 16 seconds of audio – easily sourced from public content – attackers can clone voices and manipulate victims. Executive videos and earnings calls are rich sources for voice cloning.
- **Targets Beyond the C-Suite:** Attackers now impersonate mid-level employees, not just execs. Deepfake IT staffers trick users into password resets; fake managers push urgent requests. These roles feel familiar, making their deepfaked instructions seem routine – and harder to question.
- **Adversary-in-the-Middle Kits with Deepfakes:** AiTM phishing kits now pair with deepfake voicebots. If MFA is triggered, a cloned voice – like the security head – calls the victim to deliver fake instructions, making phishing attacks harder to detect and easier to execute.

*2024 identity breach report: https://constella.ai/2024-identity-breach-report

Recommendations

Executives face a growing wave of targeted threats – from deepfakes to infostealers – making proactive identity protection critical. These steps help reduce exposure, ensure resilience, and demonstrate leadership's commitment to cybersecurity.

1

CONDUCT EXECUTIVE RISK ASSESSMENTS

Regularly audit what personal and professional data about executives is exposed online. Use internal teams or outside experts to assess breach data, social media, and web presence. Brief each executive on their unique risk in plain, non-technical language.

2

IMPLEMENT AN EXECUTIVE PROTECTION PROGRAM

Treat executive accounts as Tier 0 assets. Enforce strong authentication (e.g., physical keys), provide secured hardware, and limit work to hardened devices. Many firms now include home network security reviews, reflecting the growing need for end-to-end executive protection.

3

PERSONALIZE SECURITY TRAINING AND DRILLS

Provide tailored security coaching to executives and their assistants. Walk through likely attack scenarios like Business Email Compromise (BEC) or deepfake calls, and establish verification protocols. Assistants and chiefs of staff are often targeted, so include them in all training efforts.

4

BLEND PHYSICAL AND CYBERSECURITY EFFORTS

Ensure physical protection teams collaborate with cybersecurity. Keep travel plans secure and shared only on a need-to-know basis – attackers can exploit known absences (like long flights) to time impersonation attacks when executives are unreachable.

Summary: By wrapping your high-value personnel in an added layer of protection, you not only defend against direct attacks on them but also reinforce the overall security culture. Executives are big targets but also key allies; when they champion security (and follow it) it sets a powerful example for the whole company.

Supply Chain Identity Risk Amplifies Breach Impact

2024 saw a surge in third-party and supply chain breaches, with a growing percentage exposing not just systems but people. Vendor breaches now leak employee, contractor, and customer identities, creating identity blast radii across ecosystems. The term "supply chain attack" often brings to mind technical exploits (like SolarWinds or log4j) that cascade through software dependencies. However, an equally potent and more common variant is the supply chain identity compromise – when threat actors target a less secure partner or supplier to ultimately breach a well-defended primary organization. In 2024, these indirect attacks ramped up, showing that criminals will follow the trail of connectivity between companies, and the credentials that bridge them, to find a way in.

> Threat actors conducted large-scale campaigns, including attacks on telecoms, energy, and supply chain services – using valid credentials to silently access partner ecosystems.
>
> - IBM X-Force

Shifting from Systems to People

Historically, supply chain attacks were framed around compromised infrastructure – code, servers, and access points. This past year marked a critical shift: Attackers targeting third parties increasingly gained access to human identities embedded within partner ecosystems. Breaches now commonly expose authentication credentials, email addresses, device fingerprints, and even personal information of employees, contractors, and customers. These identity exposures don't stay siloed – they cascade across interconnected systems, enabling attackers to pivot quickly between organizations in a shared network, leaving identity as the weak link in third-party risk.

Supply chain risk is no longer just about software dependencies or unmanaged endpoints. Today, it's about who is compromised. A breached IT vendor's admin credentials can open doors across dozens of clients. An exposed executive identity in a SaaS provider can lead to sophisticated impersonation or spear phishing attacks on downstream partners. Identity now acts as the silent payload of third-party breaches, widening the attack surface beyond technical boundaries – and making detection even harder without visibility into identity exposure.

Third Parties as Gateways

Modern enterprises rely on numerous third parties: vendors, contractors, cloud services, managed service providers (MSPs), law firms, marketing agencies, etc. Each of these relationships often involves some form of identity trust: you might create user accounts for a vendor in your system, or share data with them, or rely on their platform for daily operations. **Attackers map out these interconnections and look for the weak spot.**

The recent Snowflake incident is a textbook case of identity-driven compromise. Several of Snowflake's corporate customers had not implemented multi-factor authentication (MFA), and user credentials were stolen via infostealer malware. The threat actor group UNC5537 used these credentials to access data belonging to approximately 165 companies. While Snowflake's core infrastructure was not breached, individual customer accounts were compromised. From the affected customers' perspective, this amounted to a supply chain breach – their sensitive data, stored with a third-party provider, was exposed due to identity-related vulnerabilities. In some instances, access was gained through infected contractors who had legitimate credentials to Snowflake systems. The chain was:

This illustrates that even a fourth party (a contractor of a third-party platform) can be the weakest link.

Software suppliers can introduce identity risks that go beyond code tampering. Consider platforms like GitHub or package managers: if an attacker compromises a developer's account tied to multiple projects, they could inject malicious code – classic supply chain compromise. But if the stolen credentials belong to a partner with access to a company's cloud environment or container registry, the threat becomes identity-based. In both cases, access, not just code, is the attack vector.

*axios.com

Vendor Data Breaches

Consider another angle: You secure your environment, but a vendor you shared data with gets breached, exposing your information. This happened numerous times in 2024 – perhaps most infamously with the MOVEit file transfer software breach, where the Clop ransomware group exploited a zero-day in MOVEit used by hundreds of organizations. One breach of MOVEit at a payroll vendor led to hundreds of client companies' employee data being stolen (addresses, SSNs, pay info). The result is a complex risk calculus: your security is only as good as the weakest credential among your extended network. Attackers love this because smaller firms often have smaller security budgets and less oversight, making them soft entry points. And due to the interconnected nature of business, once inside a small vendor, attackers can move upstream. We call it island hopping – going from a small island to the big mainland.

To truly manage third-party risk, organizations must go beyond access logs and vendor scorecards. They need real-time identity exposure intelligence – visibility into whose credentials are circulating, where they're appearing on the dark web, and whether those identities connect across breach ecosystems.

In today's interconnected ecosystem, your organization's security is only as strong as the weakest credential among your third-party vendors.

Recommendations

To address supply chain identity exposures, executives should champion a strategy that combines vetting, technology, and collaboration. Third-party vendors and partners often have direct or indirect access to critical systems – making their identity posture as important as your own.

1

STRENGTHEN THIRD-PARTY VETTING & CONTRACTS

Before granting access, assess vendor identity security. Embed security requirements in contracts, including audit rights and breach notification clauses. Ensure you're promptly informed if a third party suffers a breach involving your systems or data.

2

IMPLEMENT THE PRINCIPLE OF LEAST PRIVILEGE FOR THIRD PARTIES

Restrict third-party access to only what's needed. Use technical controls to sandbox their activity and conduct regular access reviews. Disable stale accounts or access no longer required – especially after projects end or inactivity is detected.

3

MONITOR AND AUDIT THIRD-PARTY ACTIVITY

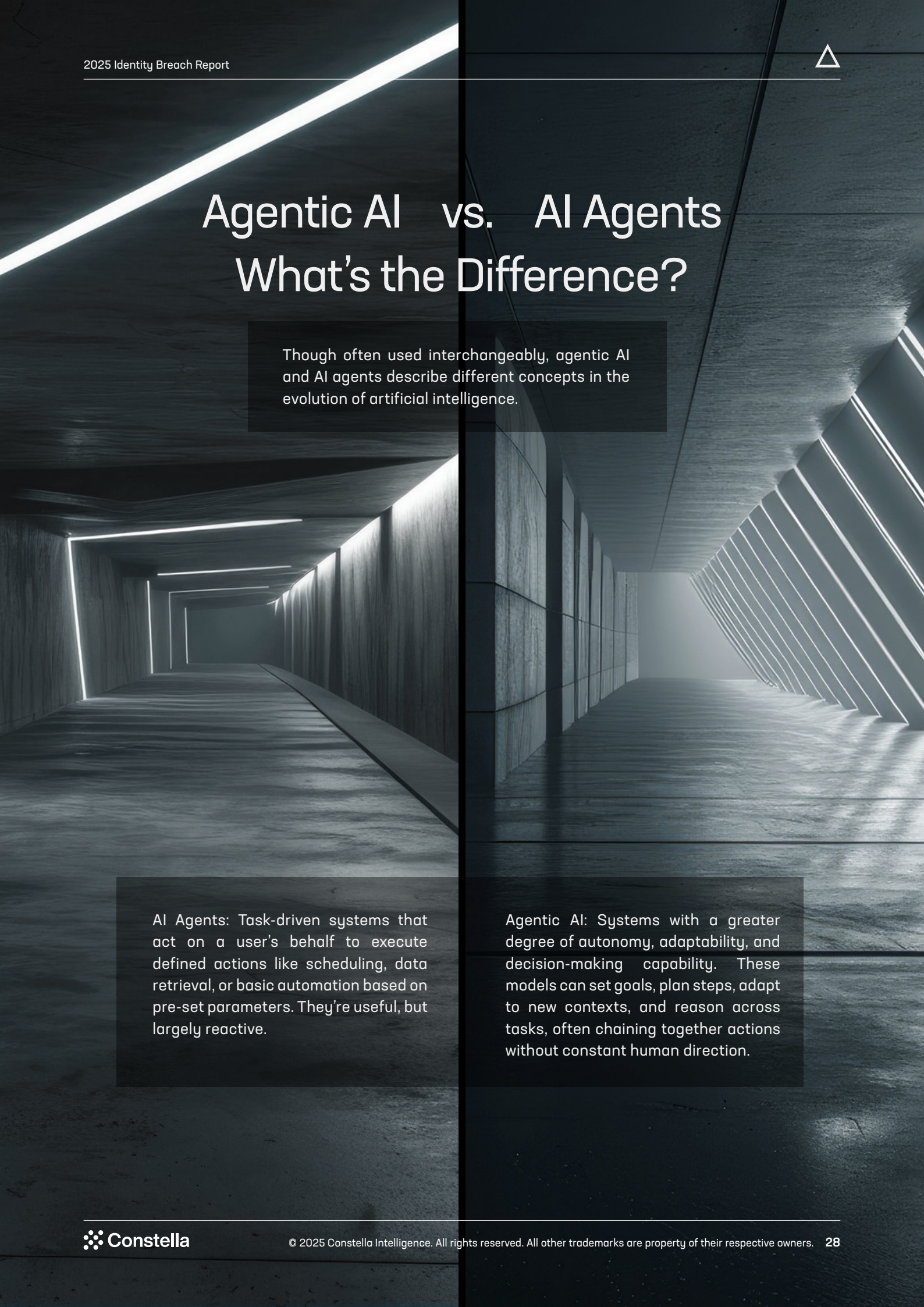
Tag third-party accounts for enhanced SOC monitoring. Set alerts for unusual access patterns and regularly audit logs. Ensure someone reviews activity and asks, "Is this normal for this vendor?" Treat third-party access with elevated scrutiny.

4

EMBRACE ZERO TRUST NETWORK ACCESS (ZTNA) FOR SUPPLY CHAIN

Adopt ZTNA to limit vendor access through authenticated, monitored gateways. Use controls like proxy access, session recording, and just-in-time provisioning to ensure vendors can't move laterally – even if their systems are compromised.

Summary: By proactively managing supply chain identity risks, organizations treat their partners' credentials and systems as an extension of their own security perimeter - one that needs equal diligence.



Agentic AI vs. AI Agents What's the Difference?

Though often used interchangeably, agentic AI and AI agents describe different concepts in the evolution of artificial intelligence.

AI Agents: Task-driven systems that act on a user's behalf to execute defined actions like scheduling, data retrieval, or basic automation based on pre-set parameters. They're useful, but largely reactive.

Agentic AI: Systems with a greater degree of autonomy, adaptability, and decision-making capability. These models can set goals, plan steps, adapt to new contexts, and reason across tasks, often chaining together actions without constant human direction.

07 Agentic AI: The Next Frontier of Threats and Defense

In cybersecurity, agentic AI can cut two ways. For defenders, autonomous AI promises faster detection and response. But for attackers, it opens the door to scalable, automated attacks that operate at machine speed and scale.

2024 gave us glimpses of how both sides might leverage agentic AI. Constella's own Andres Andreu noted that adversaries are likely to "leverage AI to craft more strategic and convincing attack campaigns ... and decentralized automation of vulnerability discovery at speed and scale."*[1] He argues defenders must move from adaptive or reactive models to models of agentic AI that proactively neutralizes threats.*[2]

> "Defenders must move from adaptive or reactive models to models of agentic AI that proactively neutralizes threats."
>
> - Andres Andreu, COO & CISO, Constella

As agentic AI becomes more accessible, organizations must prepare for a future where autonomous systems operate with greater independence – and potentially unpredictability – across digital environments. For example, we've observed AI agents conducting credential validation at scale using breached email:password combinations, paired with automated CAPTCHA-solving bots. This evolution introduces serious implications for security, oversight, and identity governance.

Dark web forums advertise access to custom AI models like "FraudGPT" and "WormGPT," trained to craft phishing emails, malware code, and even social media personas at scale.*[3] Looking into 2025 and beyond, adversaries will deploy AI agents to perform tasks like reconnaissance, password guessing, or vulnerability exploitation with minimal human oversight. Some early signs of this trend?

- In 2023, major ransomware groups were caught trying to purchase infostealer source code to integrate into their workflows *[4] – effectively blending AI-augmented data theft into their arsenal.
- Security researchers have also demonstrated AI agents that can automatically find and exploit vulnerabilities in simulated enviroment.*[5]
- Legitimate AI systems introduce new attack surfaces: In one instance, a critical remote code execution flaw was discovered in a popular AI agent framework, highlighting that AI platforms themselves can have severe.*[6]

Additionally, as identity expands in scope, it now increasingly includes non-human entities. With the rise of agentic AI, companies must manage and secure the credentials and actions of AI bots just as diligently as they do for human users.

[1] thedailypulse.net / [2] linkedin.com / [3] constella.ai / [4] axios.com / [5] sarxiv.org / [6] siliconangle.com

Recommendations

As agentic AI redefines the speed and complexity of cyber threats, security teams must act decisively to adapt. The following recommendations outline how organizations can responsibly harness the defensive potential of AI – while preparing for its weaponization by adversaries.

1

INVEST IN AI RESEARCH AND TALENT IN SECURITY

Build AI literacy across your security team. Hire or upskill staff to understand AI's role in threat detection and response. Support projects that apply AI to large-scale data, like anomaly detection in breach datasets or behavioral modeling across identity patterns.

2

PILOT AUTONOMOUS SECURITY TOOLS WITH CAUTION

Adopt AI-driven tools gradually and with guardrails. Use AI to assist with triage or recommend actions, but keep humans in the loop. Validate decisions against historical data to avoid misfires and ensure models are learning from high-quality threat intelligence.

3

SECURE YOUR AI SYSTEMS

AI models, especially those trained on sensitive or behavioral data, must be protected like any critical system. Defend against model poisoning, restrict input sources, and monitor for drift or manipulation, especially if models are tied to identity, fraud detection, or access controls.

4

CONTINUOUSLY UPDATE THREAT MODELS

Reassess threat models to include AI-enabled adversaries. Prepare for tactics like automated impersonation or deepfake-assisted phishing. Review whether your defenses and incident response workflows can withstand scaled, identity-centric attacks that blend speed, automation, and context-rich deception.

Summary: Agentic AI is a catalyst that will accelerate both attack and defense. The organizations that thrive will be those that adapt quickly, embracing beneficial AI while guarding against its malicious use.

2024 Total Metrics

Most exposed attributes, sectors, geographies, and key metadata

2024 Total Breached Identity Metrics

In 2024, Constella's threat intelligence team identified over 219K breaches containing more than 107B records and over 51B total PII attributes circulating across the deep and dark web. Other key stats are below.

219K
Breaches

Identified circulating on the deep and dark web in 2024

45.10%
Increase in total breaches over last year

55.72%
Increase in total records exposed over last year

TYPES OF BREACHES

99.33%
Breaches with PII
▲ **1.75% increase**

0.77%
Breaches with only email
▲ **0.18% increase**

0%
Breaches with only email and password
▼ **0.06% decrease**

88.98% vs. **11.02%**
Combo Breaches vs. Breaches
▲ **8.27% increase**

EXPOSED RECORDS

54.16%
Records with email
▼ **11.24% decrease**

66.37%
of those are unique emails

45.84%
Records without email
▲ **11.24% increase**

Top 20 Breaches & Leakages

In 2024, breach volumes remained high, though no incident matched 2023's REWN breach of 1.5B records. This year's largest exposures came from Tencent.com (668M) and National Public Data (647M), followed by a steep drop to 1win.com (194M). While the top breaches were smaller in size, more large-scale incidents occurred: 9 breaches surpassed 75M records, compared to 7 in 2023. The continued digitization of services and platforms expands attack surfaces, enabling cybercriminals to execute more targeted and sophisticated data leaks.

BREACHES & LEAKAGES EXPOSING THE GREATEST VOLUME OF RECORDS: 2024

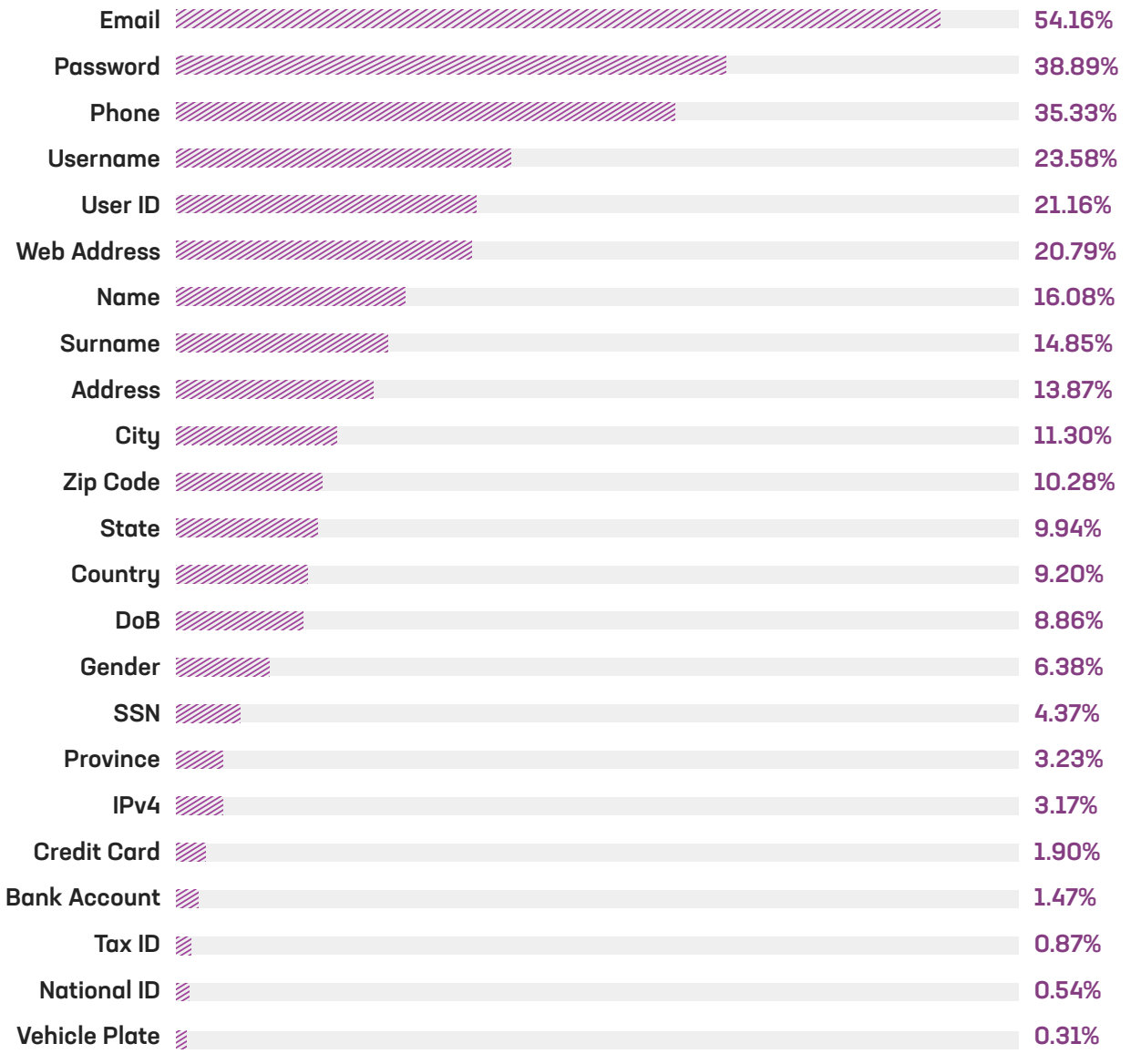
tencent.com 668M	Chinese technology and Internet services	Tencent 腾讯
National Public Data (NPD) 647M	Market research and data analytics	National Public Data
1win.com 195M	Online sports betting and gaming	1win
AT&T 142M	Telecommunications and media	AT&T
pureincubation.com 127M	Startup incubation and support	PURE INCUBATION VENTURES
thepostmillennial.com 122M	Digital media and online news	PM.
vk.com 119M	Social networking	VK
neimanmarcus.com 103M	Luxury retail	Neiman Marcus
intexmmedia.com 76M	Digital media and advertising	INTEXM MEDIA
sportmaster.ru 58M	Sports retail	СпортМастер
pureb2b.co.uk 54M	B2B digital services	PURE B2B
spasibosberbank.ru 52M	Banking and financial services	Спасибо
mtsbank.ru 50M	Banking and finance	МТС БАНК
eye4fraud.com 45M	Fraud detection and risk management	eye4fraud
eda.yandex.ru 44M	Online food delivery	Яндекс Еда
hathway.com 36M	Cable and broadband internet	hathway
vertafore.com 32M	Insurance technology	Vertafor
trello.com 30M	Project management and collaboration	Trello
cadencebank.com 12M	Banking	CADENCE Bank
lalafo.kg 9M	Online classifieds	lalafo

Top PII Exposed from Breaches

In 2024, our threat intelligence team found that emails (54%) and passwords (39%) remained the most frequently exposed data types in breaches – holding their lead from previous years but reverting to earlier percentages due to a notable rise in PII exposure overall. Phone numbers (35%) were also commonly breached, followed by usernames (24%) and user IDs (21%). Web addresses (21%), names (16%), and surnames (15%) continued to appear regularly, while bank information, as in previous years, remained less frequently exposed.

However, the increasing digital footprint and interconnected platforms continue to broaden the attack surface. With growing amounts of personal data available from open sources and underground markets, monitoring and protecting exposed PII remains critical to both individual and enterprise-level cybersecurity strategies.

BREACHES EXPOSING THE GREATEST VOLUME OF RECORDS: 2024



Top Social Media Attributes

The 2024 data reflects the number of breaches and data leaks linked to social media (SM) profiles. Among the SM attributes listed, Constella's analysts have observed Facebook profiles as the most commonly identified SM attribute exposed. Other commonly identified include Twitter, Linkedin, and ICQ profiles.

For threat actors, SM attributes can prove useful for a few important reasons:

1. Threat actors can obtain personal information about their targets, such as locations, workplaces, hobbies, family members, or friends.

2. By obtaining a victim's personal information, threat actors can launch more effective and sophisticated impersonation attacks in efforts to obtain sensitive information. These attacks could be targeted towards several possible entities, including company of employment, bank accounts, other financial information, and much more.

Using similar methods, albeit for different objectives, security analysts and researchers can leverage these attributes to better understand the potential correlation between an email or user and a real identity, making it more efficient and easier to establish a network of connections that can aid in the identification of malicious actors.

Exposed attributes identified includes social media usernames, IDs (user identification numbers specific to a digital platform), and tokens, which can be linked to any identity inside the breach where they are exposed.

FROM 100% OF THE 2024 SOCIAL MEDIA RELATED VOLUME OF RECORDS

Top 5 Social Media Profiles

49.7%	14%	13.6%	3.9%	0.30%

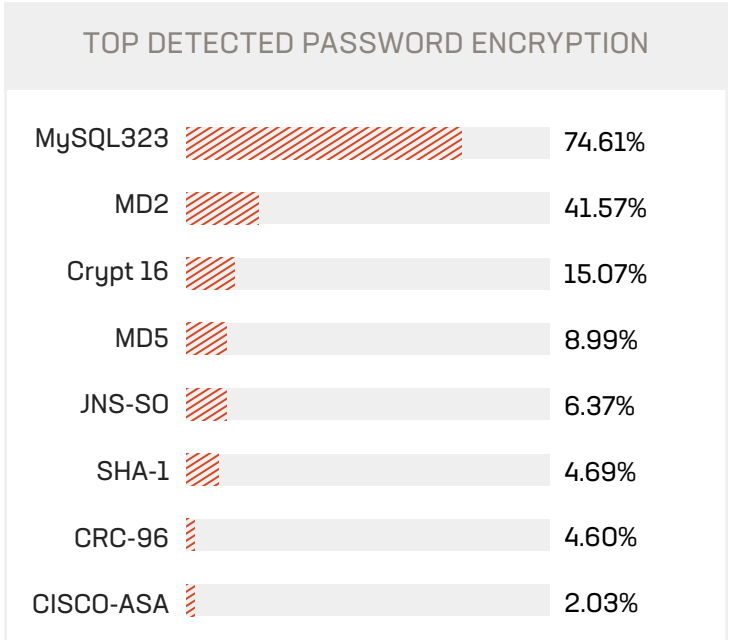
Others with less presence

Password Algorithms

The graph below highlights the most frequently detected password encryption algorithms found in the analyzed breaches. Encryption algorithms determine the complexity and uniqueness of stored passwords, making them harder for cybercriminals to crack using techniques like dictionary or brute-force attacks. Wordlists – databases of plain text passwords – are often used in such attacks, especially when unencrypted passwords are exposed.

The analysis of password algorithm usage in breaches from 2023 to 2024 reveals a concerning trend: The use of plaintext passwords increased from approximately 70.99% in 2023 to 95.29% in 2024 – a staggering rise of over 24 percentage points. This indicates that a vast majority of breached records now include passwords stored in plain text, making them immediately exploitable.

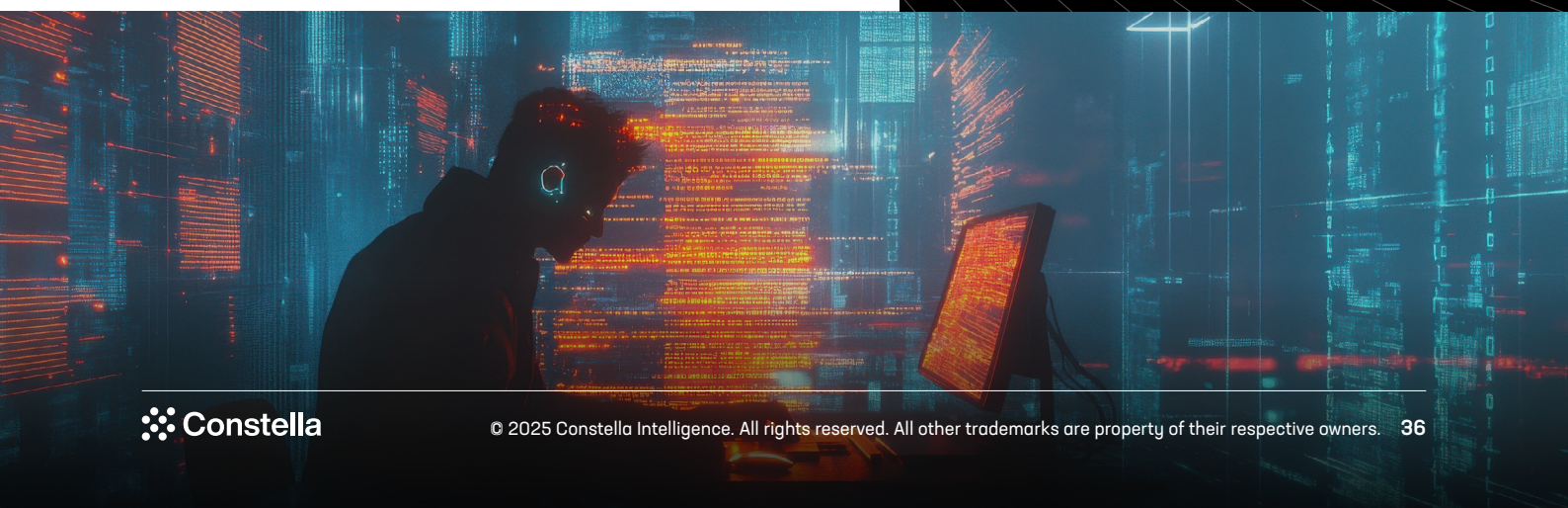
Conversely, the proportion of breaches with no passwords recorded saw a small decline, from 9.17% in 2023 to 7.78% in 2024.



95.29%

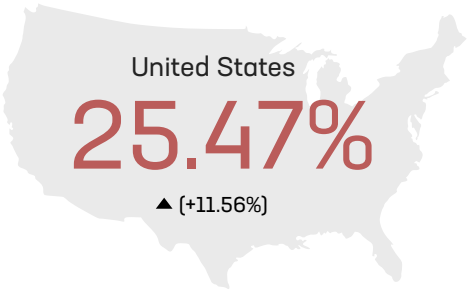
of breaches have plaintext passwords

Note: Password encryption algorithms including peoplesoft, blowfish(openbsd), phpbbv3x,wordpress, cryptocurrency(adress), dnssec(nsec3), bsdi-crypt, sha-256, md5-crypt, sha-512,cisco-ios,mysql5.x, drupal, hmac-md5, eggdrop-irc-bot, citrix-netscaler, django(pbkdf2-hmac-sha256), django(sha-1), domain-cached-credentials, sha-512-crypt, snefru-256, domain-cached-credentials-2, double-md5, drupal>v7.x, fortigate(fortios), haval-192, hmailserver, lineage-ii-c4, lm, minecraft(authme-reloaded), osx-v10.7, ripemd-256, ripemd-320, scrypt, sha-384, skein-1024, and woltlab-burning-board-4.x were identified in less than 1% of breaches.



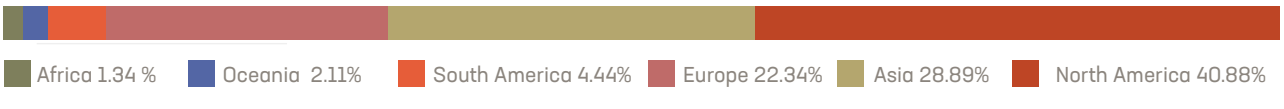
Geographic Distribution

In 2024, the United States remained significantly ahead in breach incidents, representing 25.47% of all recorded breaches, nearly doubling from 13.9% in 2023. This substantial rise highlights an increased targeting or vulnerability of U.S. based entities. Russia stayed in the second-most affected country, with breaches increasing nearly threefold to 9.9% from 3.25% the previous year, possibly reflecting intensified cyber warfare or internal cybersecurity weaknesses. Germany also shows a noticeable uptick, moving from 2.70% in 2023 to 5.07% in 2024, signifying heightened cyber threats within Europe's largest economy.



COUNTRIES MOST IMPACTED BY BREACHES IN 2024*

United States	▲ (+11.56%)	25.47%
Russia	▲ (+6.59%)	9.87%
Germany	▲ (+2.37%)	5.07%
India	▲ (+1.88%)	4.27%
France	▼ (-0.64%)	3.20%
United Kingdom	▼ (-0.80%)	1.87%
Canada	▲ (+0.40%)	1.33%
Australia	▲ (+0.40%)	1.33%
Spain	▲ (+0.06%)	1.33%
Poland	▼ (-0.01%)	1.07%
Brazil	▼ (-0.26%)	1.07%
Mexico	▲ (+0.37%)	0.93%
China	▼ (-1.12%)	0.80%
Italy	▲ (+0.18%)	0.80%
Indonesia	▼ (-1.06%)	0.80%
Peru	▲ (+0.55%)	0.80%
Japan	▼ (-0.69%)	0.80%
Ukraine	▼ (-0.46%)	0,53%
Turkey	▼ (-0.34%)	0.53%
Israel	▼ (-0.18%)	0.53%



Most Impacted Sectors

Email providers surged dramatically this year – representing 22.17% of breaches, a nearly fourfold increase from just under 6% the previous year. This rise underscores email platforms as increasingly strategic targets due to their role as gateways to broader systems and sensitive user information.

Conversely, several traditionally high-profile sectors experienced notable declines. Retail and Services each saw their percentages slashed in half, dropping to just 2.6% and 2.2%, respectively. Health also saw a similar reduction, now accounting for merely 0.5% of breaches, down from 1.1% previously.

Credential Theft with Global Motives

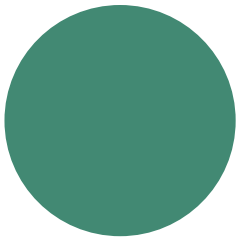
Constella data shows a sharp rise in domain-specific webmail compromises during 2024, with heavy targeting of global platforms and domains tied to Russian-linked services. Notably, six of the top ten most compromised domains are associated with .ru or Russian infrastructure, accounting for a significant share of exposed credentials.

Gmail leads with over 3.1B compromised accounts, followed by hotmail.com (1.45B), yahoo.com (1.38B), and Russian services like mail.ru (347M) and yandex.ru (121M). The inclusion of global domains like qq.com (731M) and aol.com (508M) underscores a broad, cross-border attack pattern.

These trends highlight how credential harvesting supports geopolitical cyber operations. Backed or tolerated by state actors, these campaigns exploit digital vulnerabilities at scale.

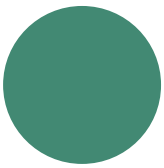
Groups like UserSec, NoName057(16), CyberArmy of Russia, and LulzSec – under alliances like the Holy League – have openly threatened institutions and Western allies, with recent attacks already impacting government assets in countries like Spain.

TOP 2024 COMPROMISED DOMAINS



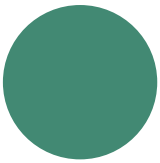
gmail.com
3,106,527,598

mail.ru
347,642,433



hotmail.com
1,450,199,267

web.de
1,384,690,115



yahoo.com
1,384,690,115

cromcast.net
161,276,828

qq.com
731,645,025

hotmail.fr
124,996,595

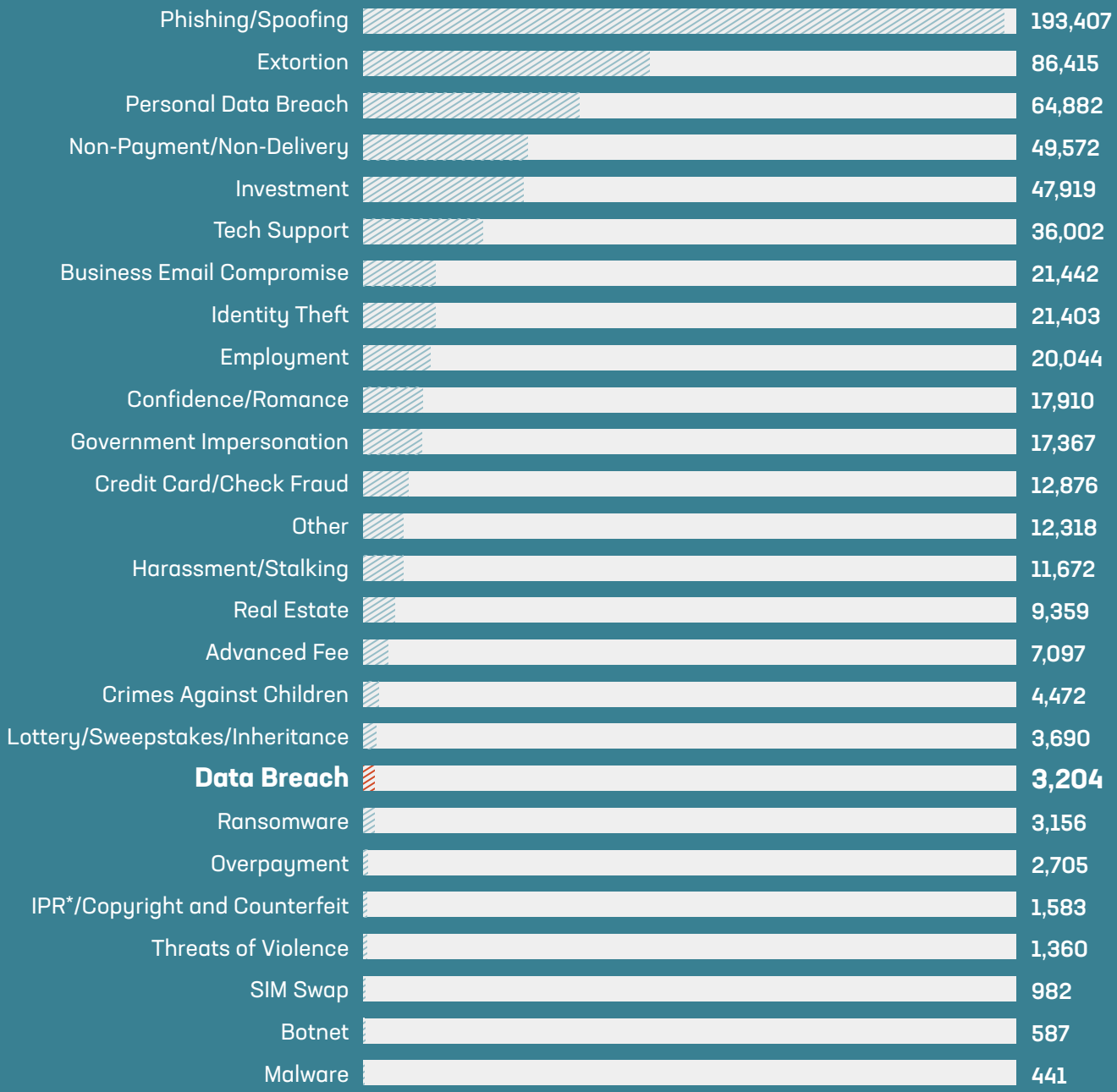
aol.com
508,167,528

yandex.ru
121,495,391

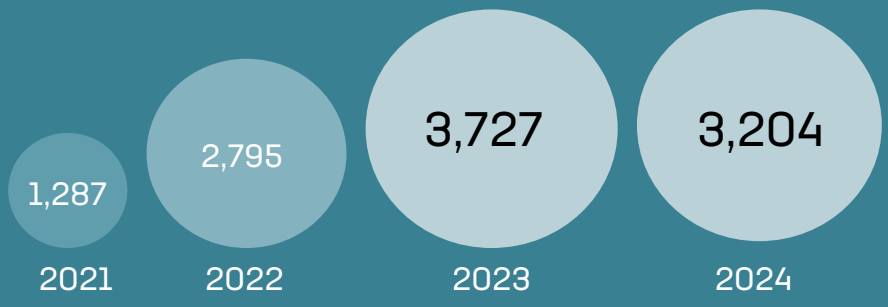
Prevalent Types of Attacks

2024 Crime Types by Complaint Count*

According to the 2024 FBI Cyber Crime Report, from a total of 859,532 complaints.



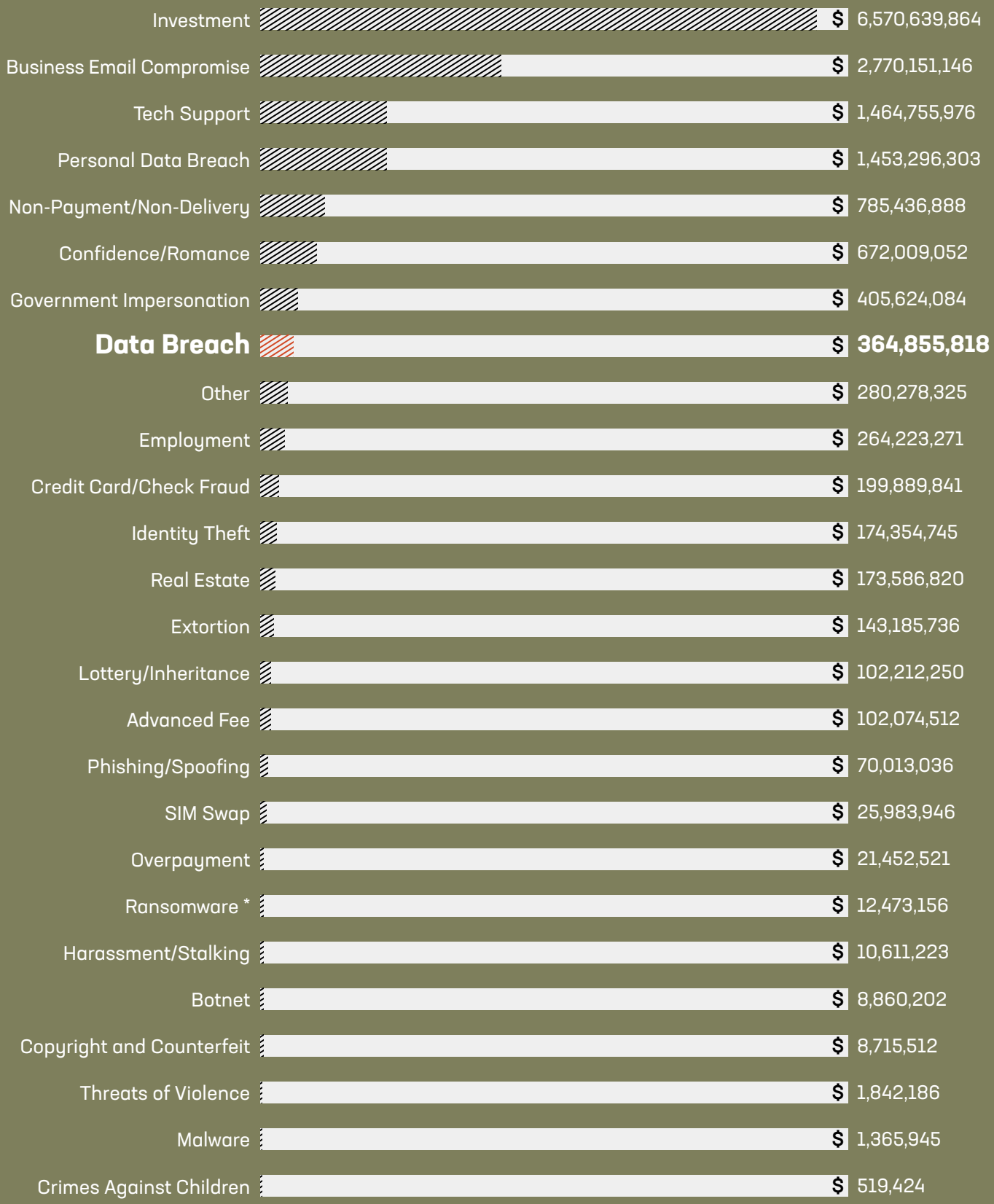
Data breaches have surged over the past three years – more than tripling from 1,287 incidents in 2021 to 3,727 in 2023, and remained elevated with 3,204 breaches reported in 2024.



* Source: Federal Bureau of Investigation: Internet Crime Report 2024 Report: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

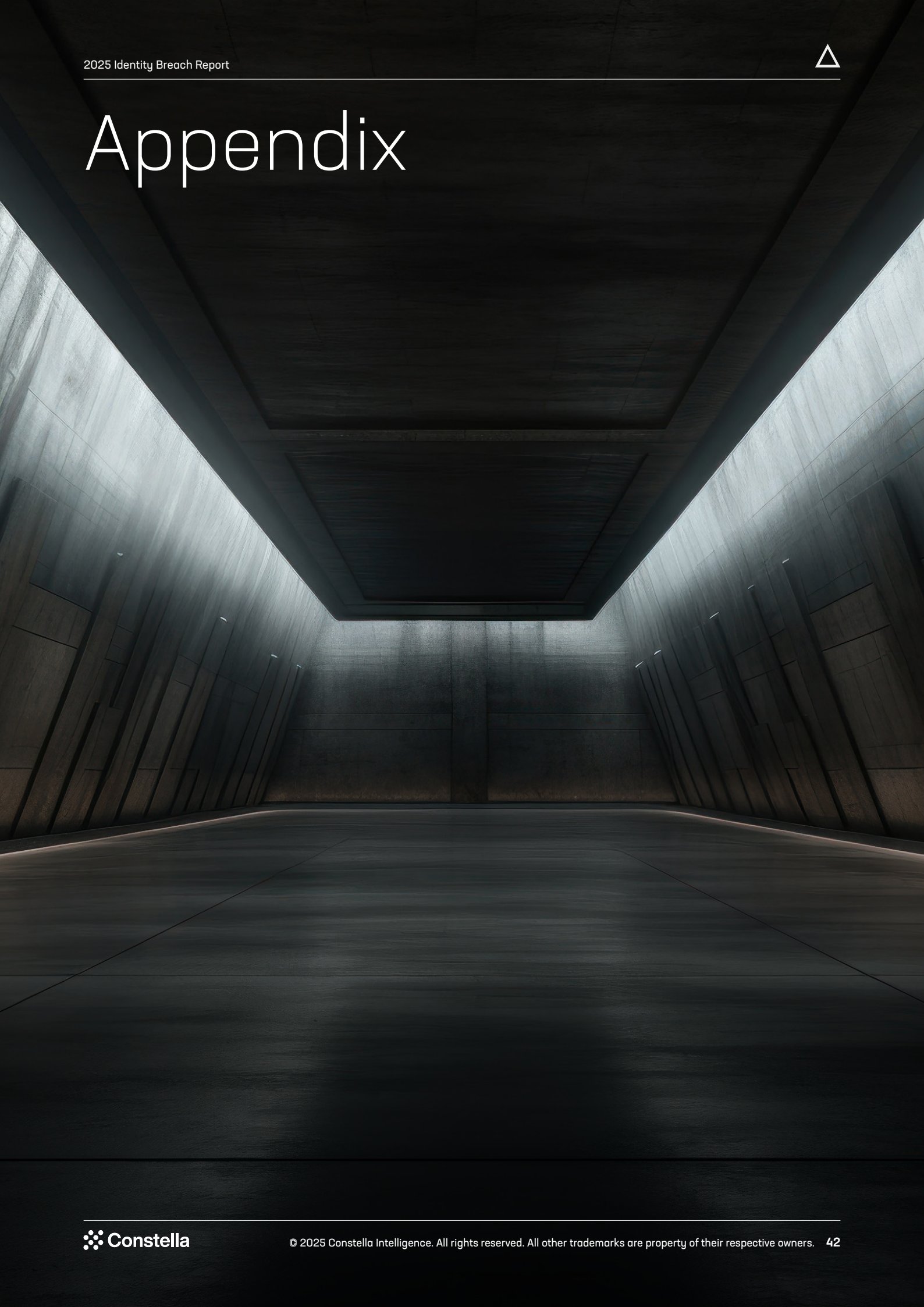
2024 Crime Types by Complaint Loss

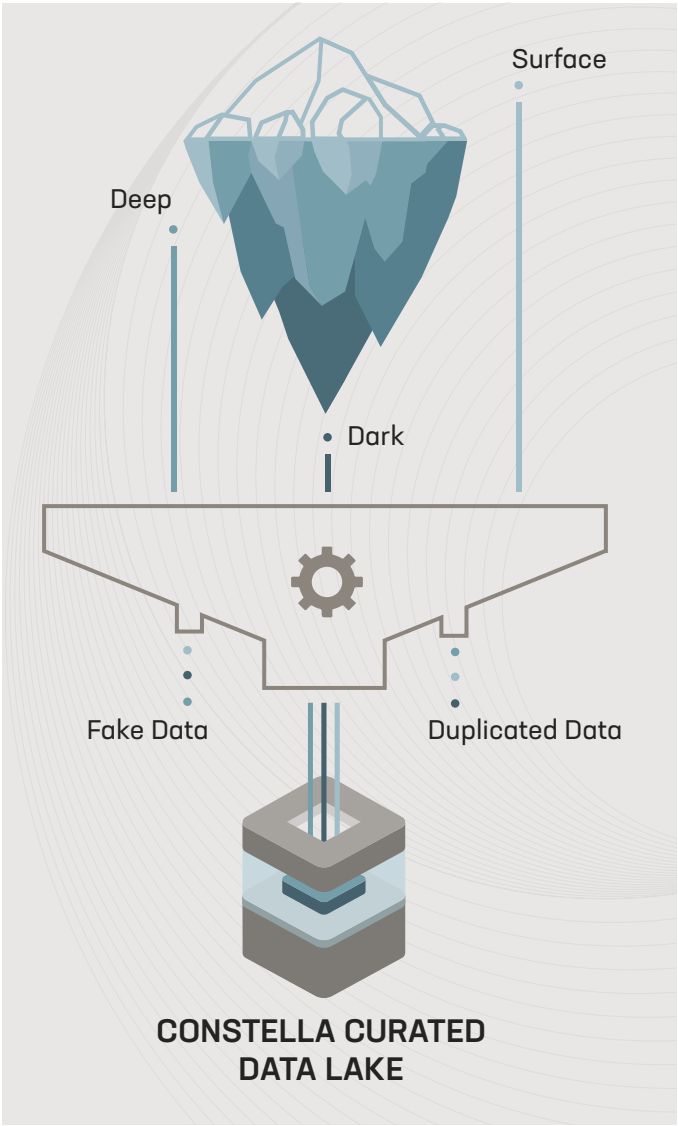
According to the 2024 FBI Cyber Crime Report, data breaches ranked 19/26 in volume of cyber crimes reported (see chart on previous page) but an astounding 8/26 in dollar value of loss - $364M. *



* Source: Federal Bureau of Investigation: Internet Crime Report 2024 Report: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Appendix





Data Sources

Constella has monitored the Tactics, Techniques, and Procedures (TTPs) of threat actors closely and developed this report based on breaches and leakages identified in 2024. In addition to the known breaches and leakages reported in the media, Constella detects information found in data dumps posted in the open, but often transient, sources in the deep and dark web. Constella's automated crawlers and subject matter experts use a variety of sources to authenticate and verify the data, including:

- **Underground communities and forums**
- **Black markets**
- **The deep web**
- **The dark web**

Constella analyzes, verifies, cleans, and attributes the data to further understand the severity of risks facing consumers and companies. Constella then alerts the impacted parties to mitigate risks. We assess the severity of risk based on multiple factors, including:

- **Sensitivity of information**
- **Authenticity of the data**
- **Number of individuals impacted**
- **Age of each type of sensitive identity attribute exposed**

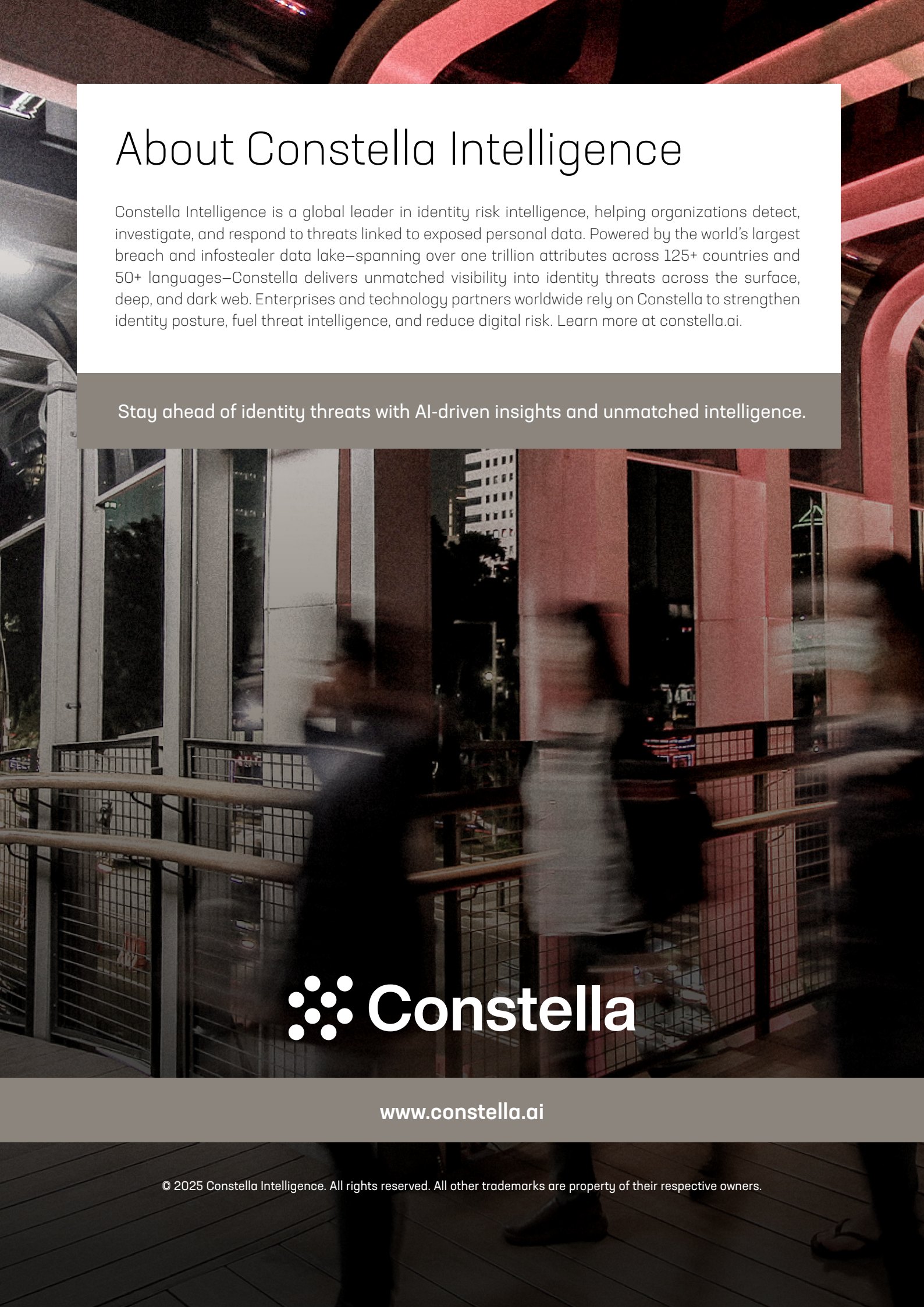
Data Verification/Methodology

While the number of accumulated raw identity records provides insight into the exposure of identity-based data, it is not the best indicator of overall risk.

This is because not all of the data gathered is authentic or unique. After collecting the raw data, Constella analyzes the details using machine learning algorithms – quickly identifying real (not fake) data, flagging sensitive information, and removing duplicate records.

Next, breaches undergo a rigorous verification process, where our analysts and experts use numerous research and investigative methods to ensure that the domain and breach information are real and valid. The breach is then attributed and normalized.

After a breach is verified, the Constella platform calculates a risk score based on several variables, including types of attributes, date, and password strength.



About Constella Intelligence

Constella Intelligence is a global leader in identity risk intelligence, helping organizations detect, investigate, and respond to threats linked to exposed personal data. Powered by the world's largest breach and infostealer data lake—spanning over one trillion attributes across 125+ countries and 50+ languages—Constella delivers unmatched visibility into identity threats across the surface, deep, and dark web. Enterprises and technology partners worldwide rely on Constella to strengthen identity posture, fuel threat intelligence, and reduce digital risk. Learn more at constella.ai.

Stay ahead of identity threats with AI-driven insights and unmatched intelligence.

Constella

www.constella.ai