auth0

The State of Secure Identity 2022

Protecting Customer Identity and Access Management (CIAM) Services Against Online Threats

EBOOK

auth0.com

Contents

Methodology

This report is based on data from Auth0 customers around the world, and so represents real-world observations of identity attacks.

The data was retrieved by Auth0's security researchers, by running simple and anonymous queries against our aggregate database of operational telemetry.

Industry segmentations are based upon each customer's self-reported segment.

Foreword: Securing CIAM

Welcome to the second annual State of Secure Identity Report! In last year's Afterword, I wrote that "Identity is Trust," to mean that identity is a constant participant in security and underscores the trust granted from applications to users (and vice versa).

I believe that is even more true today. However, the technical implementation of Trust, let alone Identity, is complicated, and being informed on the threat landscape is critical to protecting both.

Last year, this report helped to drive conversations with boards and CISOs around their Zero Trust strategy, and this year, Zero Trust continues to be a major focus for companies around the globe — boosted in part by **highly influential champions.** As digital transformations continue, the Zero Trust paradigm is proving to be effective against modern and sophisticated threats, and the need for secure Customer Identity and Access Management (CIAM) is top of mind for many organizations.

CIAM is a unique segment of the wider Identity and Access Management (IAM) space, as customer-facing applications face a different threat landscape and must deliver an experience that's user friendly — as well as secure and private. While workforce identity management can accommodate comparatively higher friction and can often count on a user base that has undergone security awareness training, CIAM lacks these factors and must rely on more subtle techniques to achieve and maintain a strong security posture.

Importantly, these techniques must be continuously tuned to achieve the appropriate balance of user experience, security, and privacy — a balance that itself varies based upon each organization's risk profile and appetite.

Presented in this report are trends, examples, and observations unearthed from the Auth0 platform in the hope that bringing light to such insights will help organizations understand the threats against CIAM and to drive informed conversations around Zero Trust.

Thank you for taking the time to read this report, I truly hope you find it useful and enlightening.

— JAMEEKA GREEN AARON, CISO, CUSTOMER IDENTITY, OKTA

Executive Summary

To maximize conversions, retention, and lifetime revenue per customer, today's application and service providers are under pressure to continually evolve the user experience (UX) they deliver.

For customer-oriented businesses, maximizing UX involves minimizing friction. However, to protect user privacy and comply with increasingly unforgiving regulatory requirements, this result must be achieved without sacrificing security — and a first step toward implementing Customer Identity and Access Management (CIAM) securely is to understand why and how adversaries are attacking these vital systems.

In this report, Auth0 shares insights from our observations and analysis to increase awareness of threats and provide strategies for mitigation. What we've seen shows:

- **Fraudulent registrations are an ever-present and growing threat.** In the first 90 days of 2022, signup fraud accounted for approximately 23% of signup attempts on our platform, up from 15% in the same period last year (per last year's report). Energy/Utilities and Financial Services experienced the highest proportion of signup attacks, with such threats accounting for the majority of registration attempts in those two industries.
- **Credential stuffing is on a record pace.** 2022 has already delivered the two largest such credential stuffing attacks we have ever witnessed and across all industries credential stuffing accounts for 34% of overall traffic/authentication events on our platform. While most industries experienced a credential stuffing rate of less than 10% of login events, in several cases — Retail/eCommerce (more than 80%), Financial Services, and Entertainment — these attacks represented the majority of login attempts.

- **Threat actors are targeting multi-factor authentication (MFA).** Because of its proven merits, more application and service providers are recommending or requiring MFA. Consequently, the first half of 2022 has seen a higher baseline of attacks against MFA than any previous year in our dataset. As attackers become more sophisticated at targeting this important defensive measure, it's critical that MFA be implemented correctly and that strong secondary factors are chosen.
- **Every company faces unique challenges.** The threats facing any particular application or service vary enormously by geography, industry, and brand prominence, among other factors. At the same time, different organizations have different risk appetites and exposures. The appropriate level of friction introduced by security measures will therefore vary on a company-to-company basis.

As adversaries focus greater attention on attacking identity systems and continue to evolve their tactics, techniques, and procedures (TTPs), it is essential for application and service providers:

- To **implement defense-in-depth** tools that work in combination across the user, application, and network layers;
- To **continually monitor their applications** for signs of attacks and changes in TTPs;
- To **make adjustments as needed** (e.g., tune parameters, tighten restrictions, introduce new tools, etc.).

At the **user layer**, MFA — particularly using WebAuthn — and breached password detection (and alerting users) can significantly reduce the risk of account takeovers.

Application-layer defenses that use detection mechanisms (e.g., rate thresholds, reputation scores, impossible travel, bot detection) in combination with continuous authentication techniques, adaptive MFA, and step-up authentication are essential for combating ever-more-sophisticated attacks without introducing unnecessary friction.

At the same time, **network-layer defenses** including allow/deny lists and Web Application Firewalls (WAFs) still have a role to play — provided they aren't used in isolation and that their limitations are recognized.

Getting CIAM right — that is, implementing it in a scalable manner to satisfy the concurrent needs of user experience, security, and privacy — is a challenge for every organization:

- Because **CIAM sits at the heart of customer-facing systems** — serving as an input into market analysis and influencing acquisition, conversion, and retention efforts — it aligns with marketing and customer experience departments.
- At the same time, **CIAM has a significant role to play in security and privacy**, putting it squarely in the sights of CISOs, CIOs, and compliance officers.
- And — fundamentally — **CIAM is a set of technology solutions**, causing it to fall under IT organizations, or even CTOs (when properly regarded as an enabler of digital transformation).

Leaders across these functions should work together to implement CIAM in a manner that balances quality of customer experience and system security, in the context of desired use cases, customer types, data types, industry-specific risks, and risk appetite.

For most organizations, an agile, secure-by-design CIAM solution is the most effective and efficient approach, as it will allow them to tailor customer identity and access management — and continually tune as needed — without drawing in resources better applied toward advancing core competencies.

Introduction to Identity Security

Today's companies must enable their customers to engage with their apps or services at any time, from any device, in a secure and safe manner. At the same time, companies must also ensure that these engagements are convenient and consistent, across the full range of digital channels.

Modern customer identity and access management (CIAM) solutions empower organizations to balance convenience, privacy, and security for every type of user who needs access to their applications and services. CIAM also allows companies to continually evolve the user experience (UX), minimize the demand on developers for identity-related capabilities, and meet regulatory and security requirements.

In identity terms, the three essential features of an effective CIAM solution are authentication, authorization, and identity management:

- **Proper authentication** ensures that the users logging into accounts are who they say they are.
- **Effective authorization** helps businesses to provide a user with the appropriate level of access to an application and/or resources.
- **Comprehensive identity management** allows administrators to update user access permissions and implement security policies; this feature also enables customers to manage — to the the extent permitted by the use case and required by regulations — their own identities, data, and preferences.

As perimeters dissolve and Zero Trust gains adopters, identity takes on even greater importance

When something goes wrong with identity, it has the potential to go catastrophically wrong — which means securing identity is critical both to maintaining a strong cybersecurity posture and to preserving an application provider's reputation.

While the importance of identity within an organization's security posture has been clear for many years, the digital rush has accelerated timeframes by dissolving security perimeters with unprecedented swiftness.

At the same time, the Zero Trust paradigm has risen to prominence, placing even greater dependencies upon the sanctity of identity systems.

As a result of these shifts, attackers are focusing efforts on gaining access to accounts (and their rights, privileges, and information) for direct use or resale.

For example, Verizon's **Data Breach Investigation Report (DBIR) 2022** revealed that:

- Almost half of data breaches start with stolen credentials, making account takeover the number one threat for employees and customers;
- Over 80% of the breaches involving attacks against Web Applications can be attributed to stolen credentials; and
- The top two data types exfiltrated by attackers are personal data and credentials.

This focus has major consequences for organizations of all sizes, who incur costs to investigate and remediate abuse and who face severe regulatory penalties and reputational damage should a data breach occur.

CIAM is at the vanguard of identity security

While the literal definition of CIAM has remained consistent, its true meaning — in terms of what use cases it enables, using what functional components, for what types of organizations — has evolved, especially in recent years. Today, CIAM is essential for:

- **Serving consumer customers:** In the business-to-consumer (B2C) world, an effective CIAM implementation enables you to offer highly personalized promotions and recommendations that drive additional revenue and create more value for your customers — all while ensuring a convenient user experience across your digital channels.
- **Empowering business customers:** Countless organizations rely on business-to-business (B2B) SaaS applications as essential enablers. However, different users within each organization need different levels of access to different resources, and creating a convenient and secure experience requires precisely managing identity and access privileges. CIAM provides the answer by empowering B2B SaaS customers to self-manage identity.
- **Enabling constituents, partners, and other known third parties:** In consumer and SaaS applications, customers manage their own identities, but there are many scenarios where identity must be managed by the organization providing the service. To fulfill use cases where customer identities are known to, and provisioned by, the service provider, CIAM provides all the tools organizations need to manage customer account creation, maintenance, and end of life.

In an enterprise environment, security trumps convenience, so administrators can impose controls with comparatively little regard for the user experience — but customer identity management must maintain security and privacy while minimizing friction. Because of this restriction, CIAM exists at the vanguard of identity security and innovation, as it depends upon defenses that can withstand sophisticated threats but that are nearly invisible to users.

With this report, we aim to increase awareness of both threats to customer identity and the techniques that can be layered to build reliable defenses.

Friction is revenue's natural enemy

In a CIAM context, "friction" refers to anything that slows down a person's interactions with your service. These interactions may include (but are not limited to) a user:

- signing up for your service;
- logging in to their existing account;
- updating their information and preferences;
- recovering lost account data; and
- checking out (i.e., completing a purchase).

Friction is a major obstacle to user experience, conversions, and revenue. The more friction there is — in any and every customer interaction — the lower your conversion rates and the less revenue you get over both the short and long term. For example, **83% of consumers report that they've abandoned their cart or sign-up** due to an arduous login process.

Part 1: Attacks Against CIAM

Attacks that leverage or target CIAM services come in many forms, from precision “hands-on-keyboard” (i.e., manually operated) efforts to large-scale approaches that employ extensive automation capabilities and brute force tactics.

Whether threat actors seek to profit by directly abusing the rights, privileges, and information associated with accounts or instead intend to sell access, the strategic objective of identity attacks is to enable one of two outcomes:

- **Fraudulent Registration:** the attacker creates puppet accounts.
- **Account Takeover (ATO):** the attacker gains access to accounts that already exist.

One of the major objectives for consumer-facing companies is to convert prospects into first-time customers, and this makes sign-up fraud especially problematic for at least a couple of reasons:

- First, entire customer flows are often optimized based upon analytics data that shows how users interact with a user interface and ultimately ‘convert’ — but fraudulent registrations pollute this data, significantly complicating business analytics activities.
- Second, to maximize conversions, consumer businesses especially must minimize friction during the registration process — but lowering barriers for legitimate users also lowers the barriers for abusers.

Other consequences of sign-up fraud include:

- Loss of legitimate users and the associated benefits;
- Reputational damage;
- Direct financial loss; and
- Operationally expensive clean-up (and the opportunity cost of doing so).

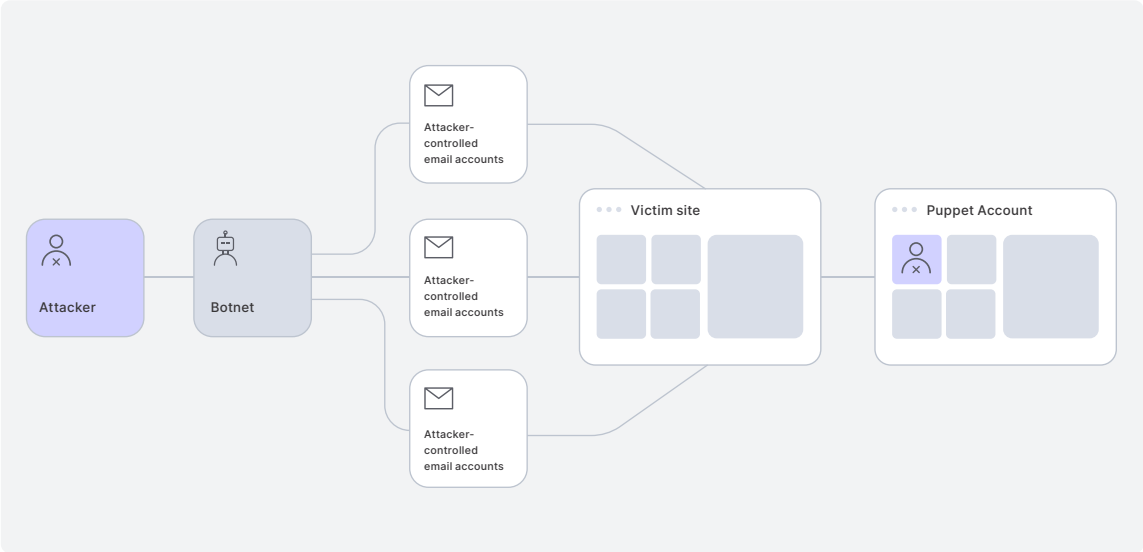
Account takeover poses a greater threat to security and privacy. In addition to attackers gaining access to resources (e.g., loyalty points) and privileges (e.g., ability to make purchases, especially of products in limited supply), they may also acquire valuable demographic and personally identifiable information (PII) — with potentially severe regulatory and contractual penalties for the organization, along with a loss of trust from users.

Let's now examine how adversaries attack identity services and the prevalence of such incidents.

Fraudulent Registrations

In a fraudulent registration attack, also known as a fake account creation attack, a threat actor abuses the account registration process to create puppet accounts.

Figure 1: Anatomy of a fraudulent registration attack



There are a number motivations for doing so, including:

- **Gaining inequitable access to something valuable,** like limited edition sneaker drops, new video game consoles in short supply, etc.;
- **Receiving awards or incentives that are associated with account creation,** including gift cards, cryptocurrency tokens, etc.;
- **Spamming, disinformation, or hacktivism campaigns** that leverage accounts to participate in comment threads or to amplify messages;
- **Committing synthetic identity fraud,** which often leverages financial services and utilities accounts;
- **Reselling accounts** to interested parties;
- **Harming the application provider's ability to deliver services** by exhausting the namespace of potential users, and thereby preventing legitimate users from registering; and
- **Optimizing ATO attacks** by using the puppet accounts to carefully manipulate login success and failure rates to bypass automated security measures.

The attacker may seek to create only a relatively small number of puppet accounts or could employ a botnet to automate the creation of thousands or even millions. In the latter case, the operation may be aided by lists of common usernames.

A sudden surge in failed signups (or the failed signup rate) is a strong indicator that your application is under attack. In this situation, you may wish to take a closer look into the registration traffic to see if thresholds or rules should be modified.

Example: A cryptocurrency promotion attracts the wrong kind of attention

Figure 2 shows account creation activity for a United States-based company involved in cryptocurrency. Like many such organizations, this company offers an incentive to entice new users to sign up.

In this case, the incentive program attracted the attention of a threat actor, who attempted to sign up huge numbers of accounts. There are a few potential motivations for doing so, including:

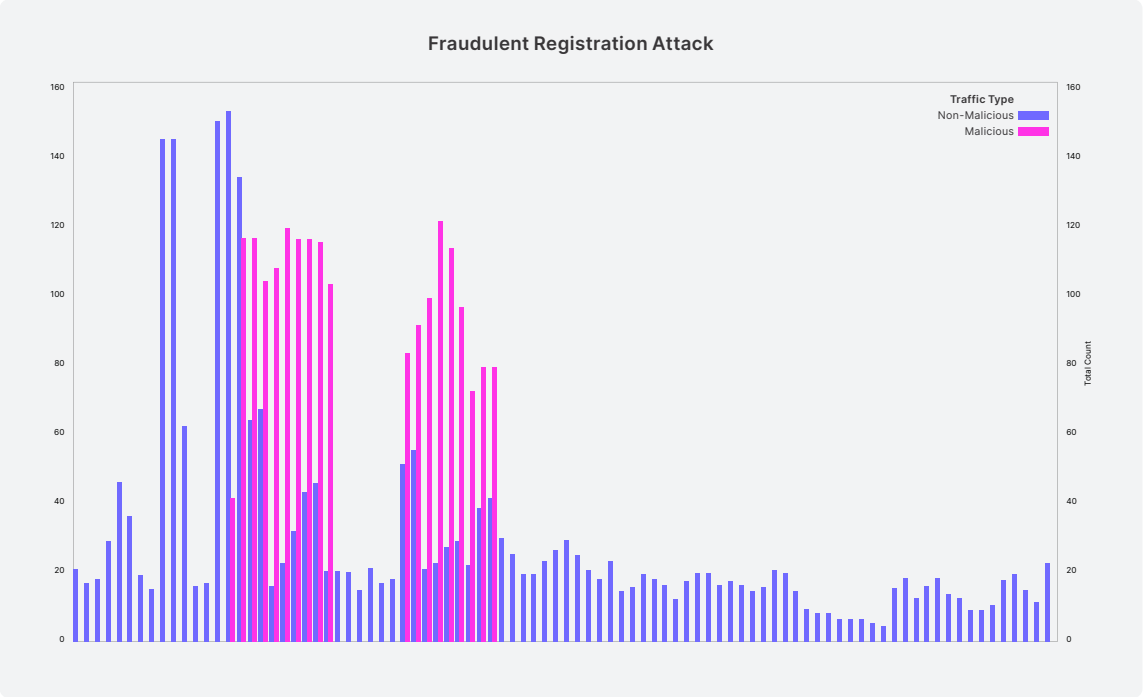
- Acquiring crypto tokens directly;
- Using the accounts for money laundering; and
- Reselling the accounts.

While the giveaway in this instance was cryptocurrency, practically any signup incentive, in any industry, has the potential to attract the attention of attackers.

The detailed characteristics of the attack clearly indicate that the threat actor leveraged bots in combination with bulk lists of pre-existing email addresses. Over nearly a month, two attack phases bombarded the service with fraudulent account creation attempts. During the attack, the number of fake signups outnumbered legitimate ones by a ratio of roughly three to one.

In this incident, the two attack phases were executed with similar tactics; however, it's not uncommon for us to observe a threat actor launch a 'reconnaissance' phase to test defenses and inform tactics to be used in a subsequent, larger-scale attack.

Figure 2: Motivated by the prospect of crypto tokens, a threat actor launched a two-phased attack



Aggregate Observations

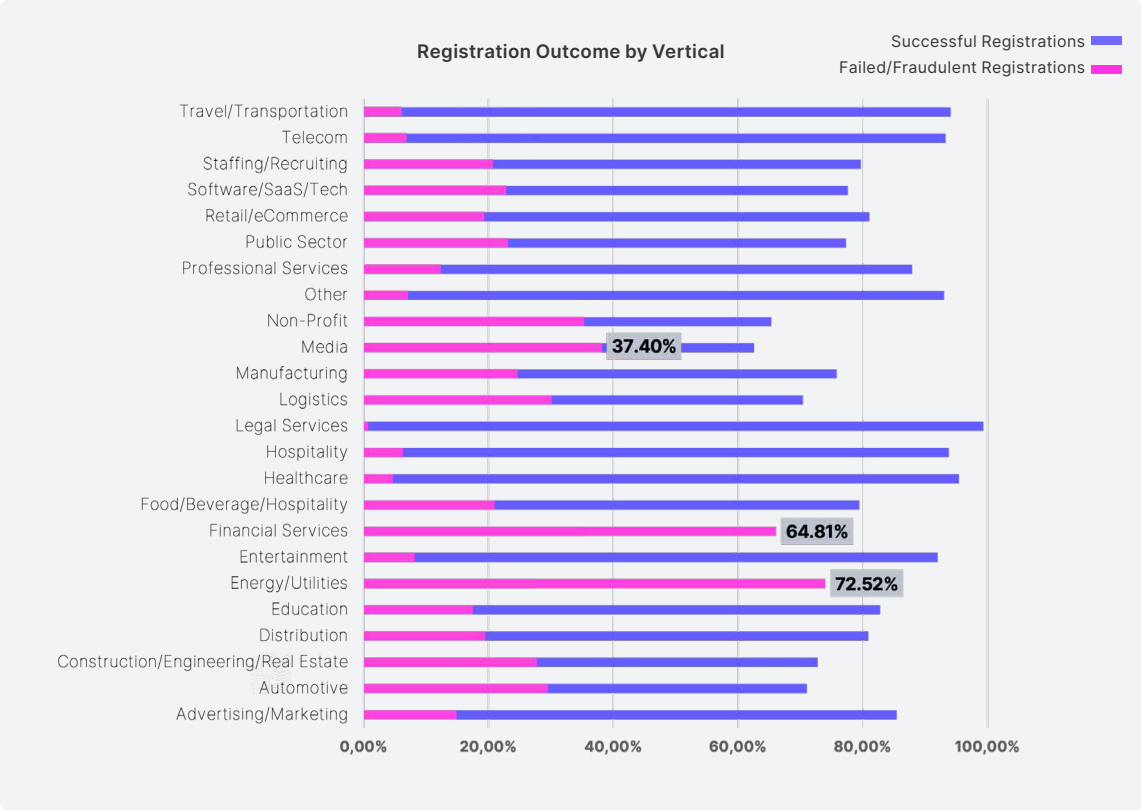
Figure 3 shows that signup fraud is an ever-present threat across all industries, albeit with considerable variation by vertical.

In the first 90 days of 2022, Auth0 observed almost 300 million fraudulent account creation attempts on our identity platform, accounting for approximately 23% of signup attempts — up from 15% in the same period last year — and 1% of overall traffic/authentication events.

While there are legitimate reasons why a genuine user might experience a signup failure, automated scripts exhibit behavior that is fairly distinct. For example, to contribute to the registration failure percentage in Figure 3, the IP associated with the signup must have experienced more than ten failures on that day — a fairly conservative threshold that is unlikely to be crossed by a genuine user.

Energy/Utilities and Financial Services experienced — by far — the highest proportion of signup attacks, with such threats accounting for the majority of registration attempts in those two industries. Exactly why these two stand apart is unknown, and both cases represent a departure from what was observed during the same period in 2021.

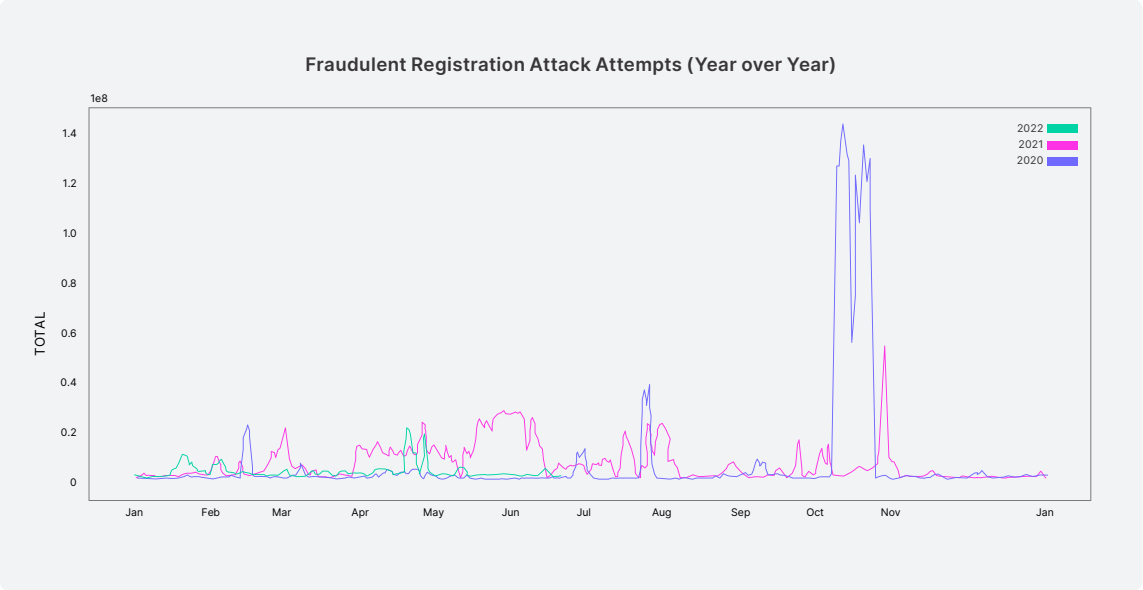
Figure 3: Fraudulent registration rates by industry during the first 90 days of 2022



Previous years (Figure 4) are characterized by a generally consistent level of fraudulent registration punctuated by sudden and significant spikes (including an enormous one in 2020), some of which turn into surges that may last up to a few months.

Seen in this context, the first half of 2022 doesn't stand out as abnormal.

Figure 4: Fraudulent registrations are an ever-present threat within CIAM



Credential Stuffing

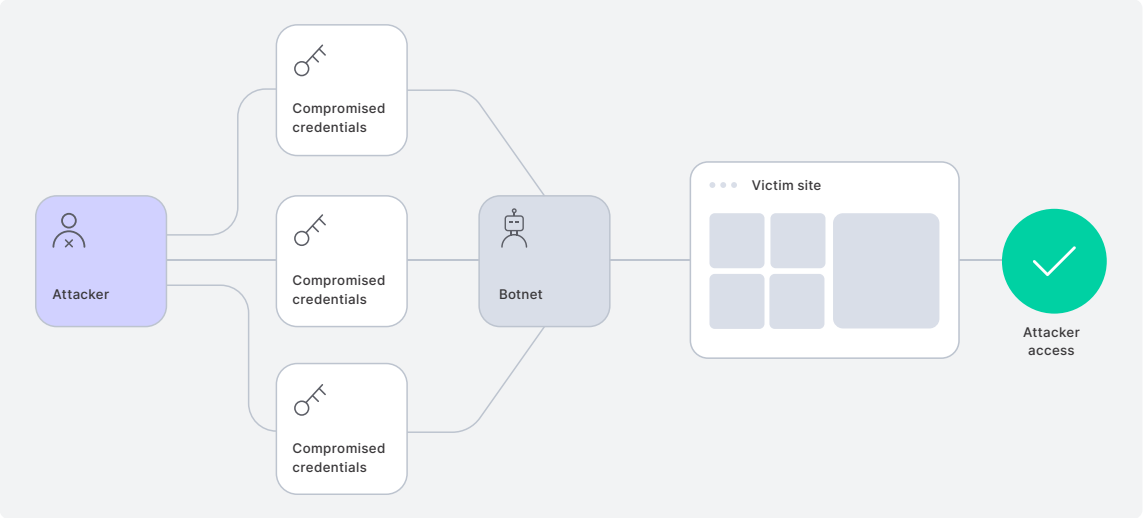
Credential stuffing attacks take advantage of the entirely too-common practice of password reuse. When an account holder reuses the same (or similar) passwords on multiple sites, it creates a domino effect in which a single credential pair can be used to breach multiple applications.

In addition to account takeovers, credential stuffing is often employed for account discovery/validation, the goal of which is to develop a high-quality list of credentials that can be sold (e.g., to sell streaming accounts at a lower price than the subscription rate).

Most such attacks use brute force to run through long lists of breached credentials. Unfortunately, the barrier to launching such attacks is very low:

- Aggregated lists like Collections #1-5 **are readily available**;
- Renting a botnet to execute the attack is easy and cheap;
- Rotating IP services to mask attack origins and try to evade regional filters are plentiful; and
- Automating the components into an orchestrated attack is straightforward.

Figure 5: Anatomy of a credential stuffing attack



Threat actors employ a number of tactics when conducting credential stuffing attacks:

- **Bursting:** Attempting anywhere from a few dozen up to hundreds of credentials in a short period.
- **Trickling:** Operating at a much lower rate, on the order of only a few attempts a minute.
- **Sprinkling:** Interspersing known valid credentials — for instance, from fraudulent accounts under the attacker's control — into the stream to evade automated detections by managing the failure rate.

Example: A 10x increase in login traffic

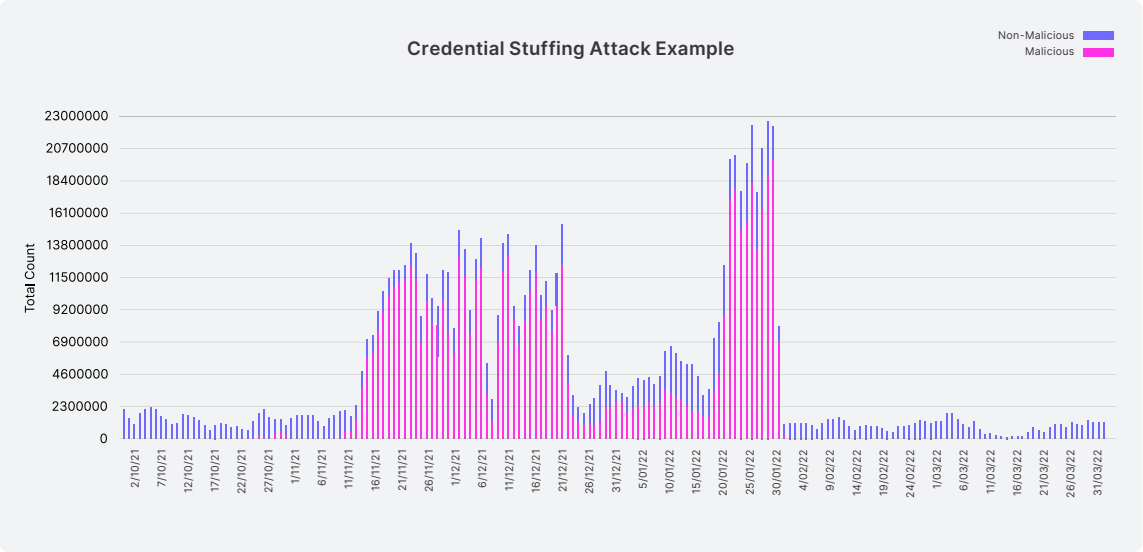
While sophisticated attackers employ more subtle tactics, most of the credential stuffing attacks we see are high volume and resemble load testing.

Figure 6 shows one such attack against a financial organization located in South America that lasted for more than two months. Within this timeframe, the credential stuffing traffic (red) was regularly 5-10 times higher than legitimate user login activity (blue).

Attacks like this one place a huge strain on the identity infrastructure, which can create latency in your application and friction for your users.

In addition to a major jump in the rate of login attempts, these incidents are characterized by sudden and significant increases in failed usernames and failed passwords; if breached password detection is in place, then you may also observe a surge in the use of known breached credentials.

Figure 6: During this sustained attack, credential stuffing traffic was regularly 5-10 times higher than legitime login activity



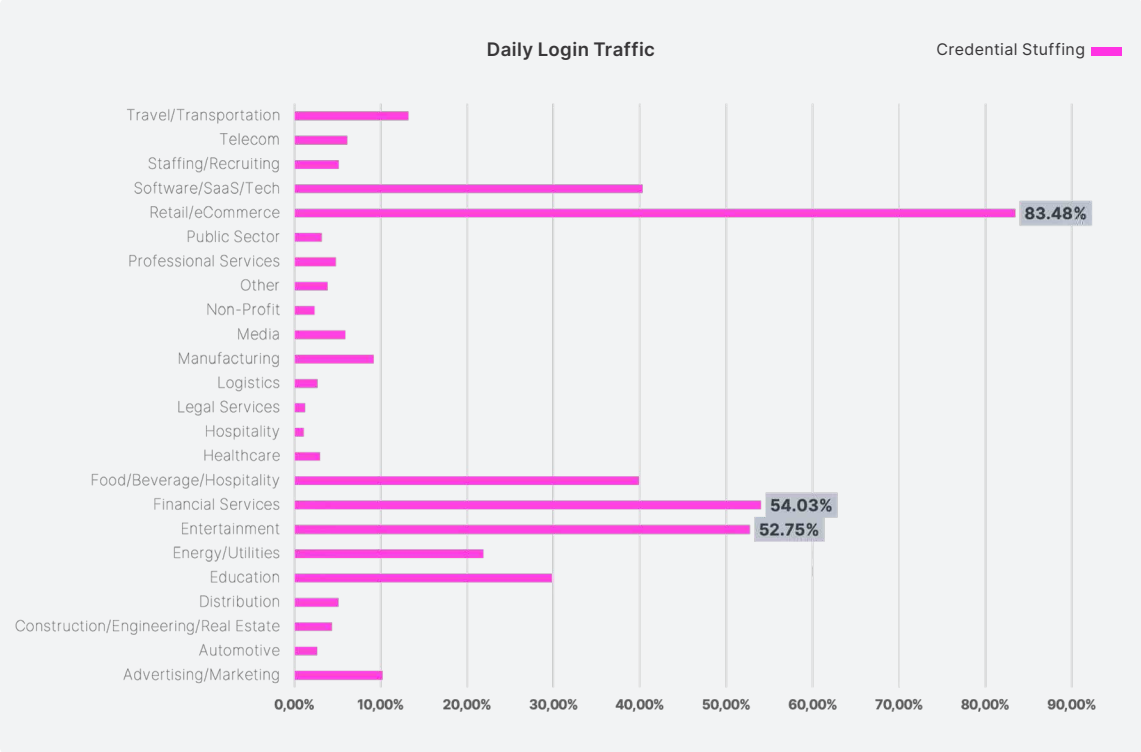
Aggregate Observations

Credential stuffing attacks are the most common threats directly observed by Auth0. In the first 90 days of 2022, we detected almost 10 billion credential stuffing events on our platform, representing approximately 34% of overall traffic/authentication events.

As shown in Figure 7, these attempts are not evenly distributed across industries. While most industries experienced a credential stuffing rate of less than 10%, in several cases these attacks represented the majority of login attempts. In Retail/eCommerce, more than 80% of observed login traffic was determined with high confidence to be credential stuffing, and Financial Services and Entertainment also both saw credential stuffing account for more than 50% of login activity.

We will also note that in this analysis we have applied a fairly conservative credential stuffing detection threshold, so these values should be considered as minimum real-world rates.

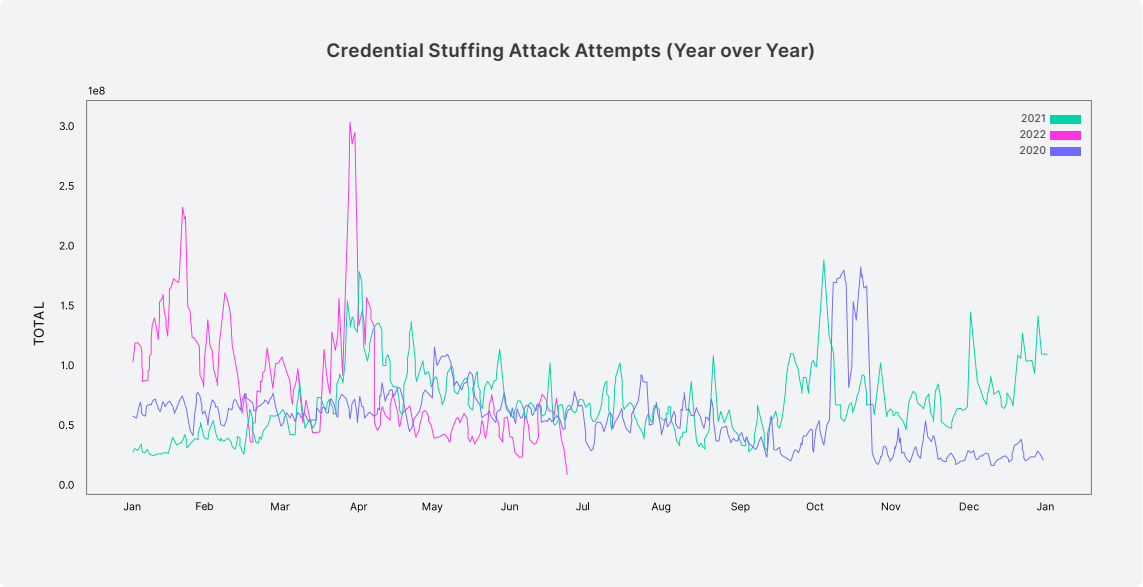
Figure 7: Credential stuffing attack attempts by industry during the first 90 days of 2022



A longer view (Figure 8) shows that the overall rate of credential stuffing attacks increased as 2021 drew to a close and that this higher level was sustained through the first few months of 2022 — including a new all-time high in mid-January. The attack rate declined to historical levels by mid-March before surging past the record set less than three months earlier.

Since the beginning of April, credential stuffing has dipped below usual levels, further illustrating the enormous variation that can occur over the span of just a few weeks.

Figure 8: Historically, credential stuffing accounts for the largest proportion of attack traffic



Multi-factor Authentication (MFA) Bypass

Application builders (and many users) understand that multi-factor authentication (MFA) is an effective way to prevent account takeovers, whether from a credential stuffing attack or from some other attack vector.

Setting aside **highly manual approaches like SIM swapping and social engineering**, to compromise an account protected by a strong MFA implementation attackers would need:

- The account credentials (e.g., from a breach or guessed before triggering an automated defense); and
- To pass the MFA challenge as a secondary proof of identity.

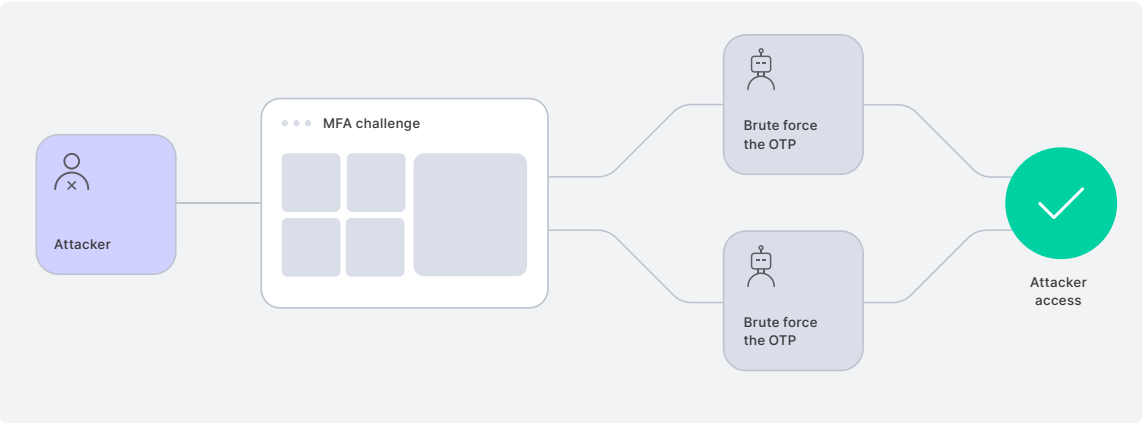
The most common attack vector is to apply brute force to either:

- Successfully 'guess' the authentication code; or
- Create 'alert fatigue' in an attempt to trick or coerce the user into completing the MFA challenge even though they didn't initiate the request.

Unfortunately, **several tools are now available** that make it easy to launch such attacks against some of the relatively weaker secondary factors — particularly SMS-delivered one-time passwords (OTPs).

We should also acknowledge that it's not uncommon for highly motivated and well-resourced threat actors to know (and to offer for sale) workarounds to MFA — particularly for corporate targets. These bypass mechanisms often leverage vulnerabilities in legacy authentication protocols, highlighting the necessity of disabling such systems and of requiring administrator approval for OAuth and similar applications.

Figure 9: Anatomy of an MFA bypass attack



Example: Looking for travel rewards, or something more?

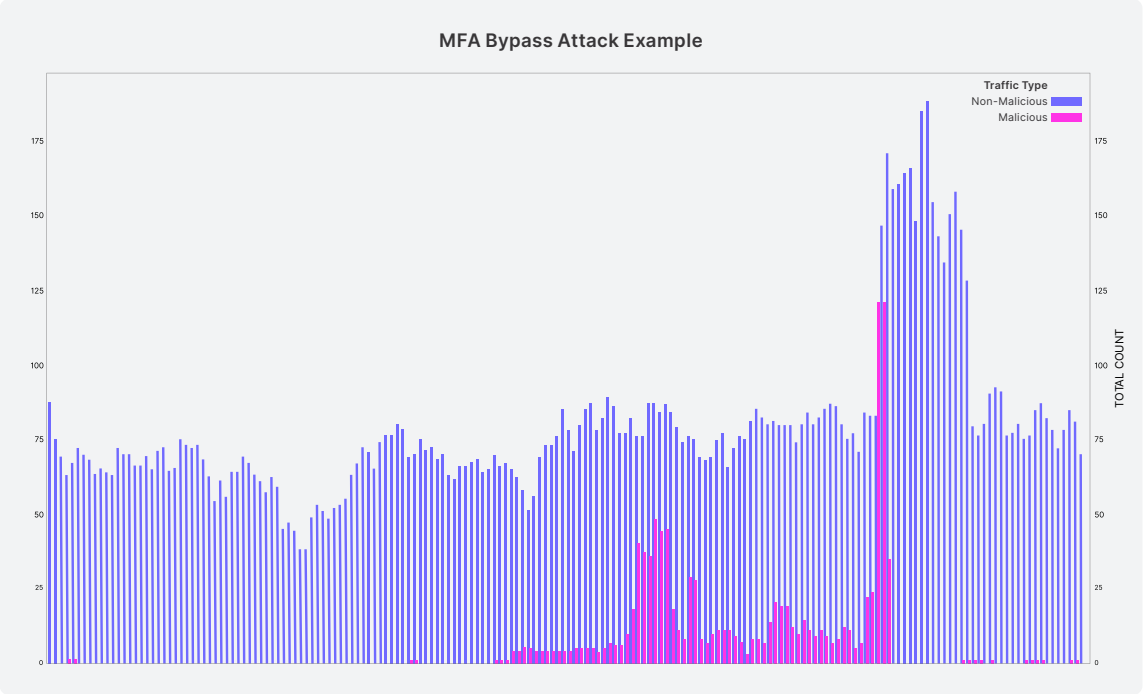
Figure 10 shows the malicious events that were part of a nearly month-long attack against a travel site aggregator/marketplace based in Europe. In this incident, the threat actor was trying to gain access to existing accounts.

While the most likely motivations are to access reward points or to resell the accounts, travel sites often hold a wealth of personal information (e.g., travel rewards account numbers, passport number, date of birth, address, etc.) and could conceivably be used to track a person's movements.

Whether by coincidence or design, the attack occurred in the lead-up to a holiday weekend (which is responsible for the surge in non-malicious traffic) in a few European countries and targeted exactly 50 phone numbers, each of which received over 100 SMS MFA codes between January 31, 2022 and February 24, 2022. The large jump in malicious traffic at the end of the attack could represent a last-ditch effort to compromise the targeted accounts, suggesting a high degree of motivation on the part of the attacker.

Consider how a user might behave in that situation: Would they recognize the onslaught of MFA requests as the signs of an attack, or would they think that the service was simply being 'buggy'? Would they approve a request or perhaps change their configuration to turn off MFA? If their credits or money were fraudulently used — or, worse, if their home was burgled while they were traveling —then would users assign blame to the travel aggregator even if their own actions directly contributed to a successful account takeover?

Figure 10: In the lead-up to a travel weekend, this sustained attack targeted exactly 50 phone numbers with more than 100 SMS MFA codes each



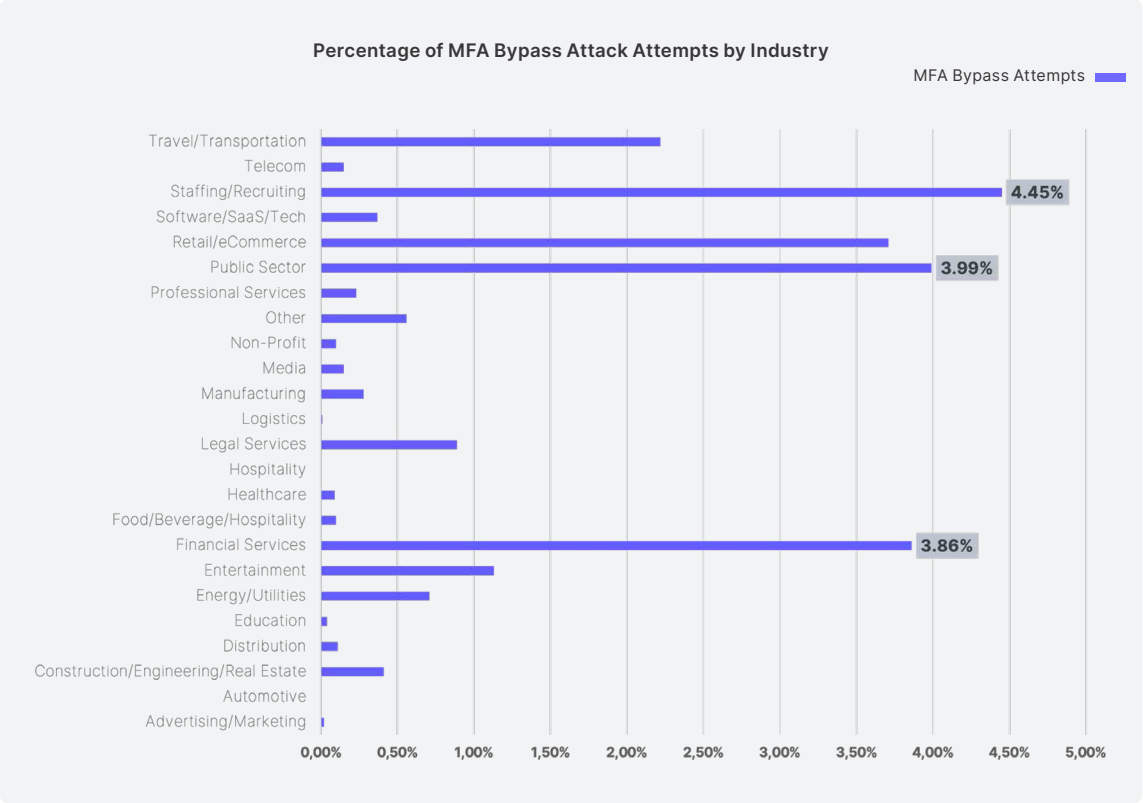
Aggregate Observations

In the first 90 days of 2022, Auth0 observed almost 113 million attacks against MFA. Because of the effort required to successfully bypass MFA, such attacks tend to focus on high-value targets. Indeed, examining the

attack rate across industries (Figure 11) shows that threat actors are focusing their attacks on Staffing/Recruiting, the Public Sector, Retail/eCommerce, and Financial Services.

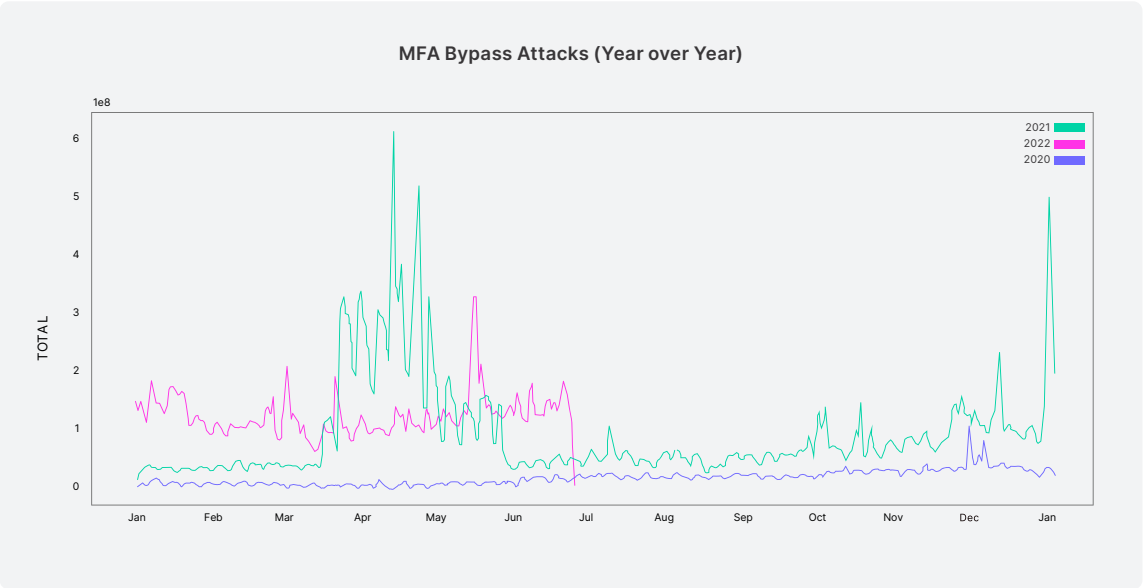
Note that to be considered a brute force attack against MFA within this analysis, during signup or authentication a user must enter an incorrect OTP more than the limit prescribed by the application provider — which is distinct from (and a much higher bar than) simply abandoning the login attempt.

Figure 11: Percentage of MFA bypass attack attempts by industry during the first 90 days of 2022



The rate of observed MFA bypass attacks trended upward as 2021 drew to a close, and included a major spike at the end of December. The first half of 2022 has seen a higher baseline of attacks than any previous year in the dataset — possibly driven by the new attack tools — although a return to previous levels at the end of June could be a reason for optimism.

Figure 12: Percentage of MFA bypass attack attempts by industry during the first 90 days of 2022



Other Notable Identity Attacks

While the threats outlined previously represent the vast majority of the attacks we observe, there are several others that warrant brief examination.

Session Hijacking

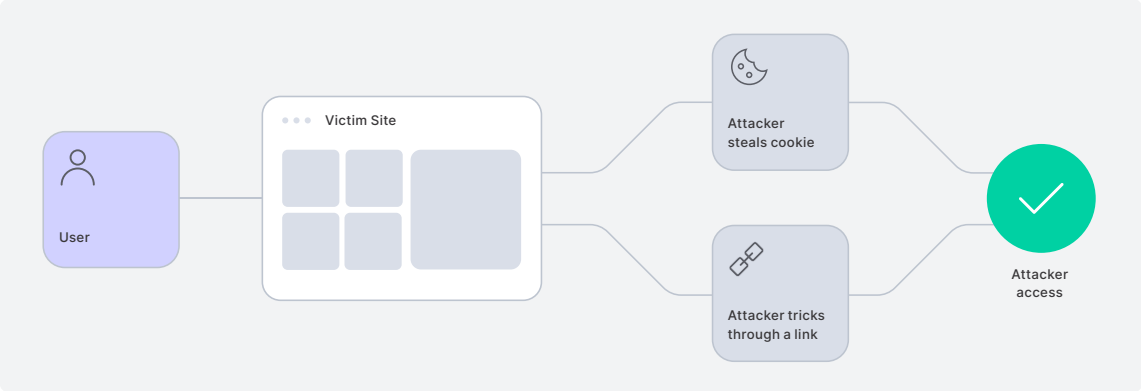
In a **session hijacking attack**, an attacker gains access to an active session without having to provide a password. The attacker maintains access as long as the session remains active (a period that varies by application provider).

Two ways to achieve this outcome are:

1. After a legitimate user logs in, the attacker steals the user's session cookie.
2. The attacker tricks the user into logging in through a malicious link with a prepared session ID.

Both approaches can be scaled somewhat, but session hijacking is more likely to be used as part of a targeted attack against particular users.

Figure 13: Anatomy of a session hijacking attack



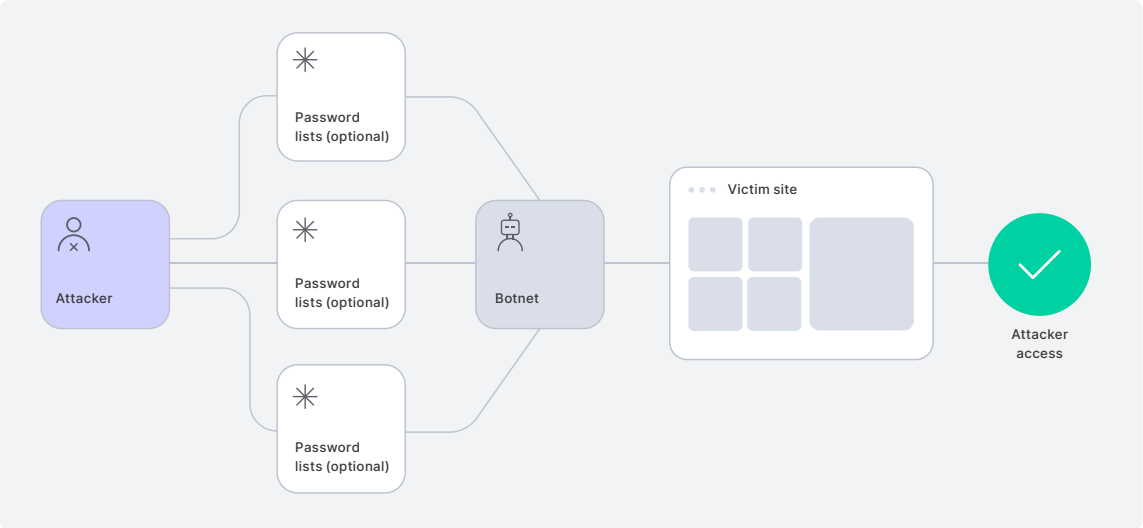
Password Spraying and Password Guessing

Password spraying is a brute-force attack method in which a threat actor uses automated tools to try common passwords across many different accounts.

Password guessing is a cruder approach: where password spraying tries relatively few passwords across relatively many accounts, password guessing tries many passwords across any number of accounts.

Because of insecure password habits (e.g., password reuse, using common words, etc.), a small number of optimizations — including leveraging lists of breached passwords and dictionaries of words that are frequently used — can dramatically improve an attacker's likelihood of trying the correct password (or, more accurately, of trying **a password that hashes to the same value as the correct password)**.

Figure 14: Anatomy of a password spraying attack

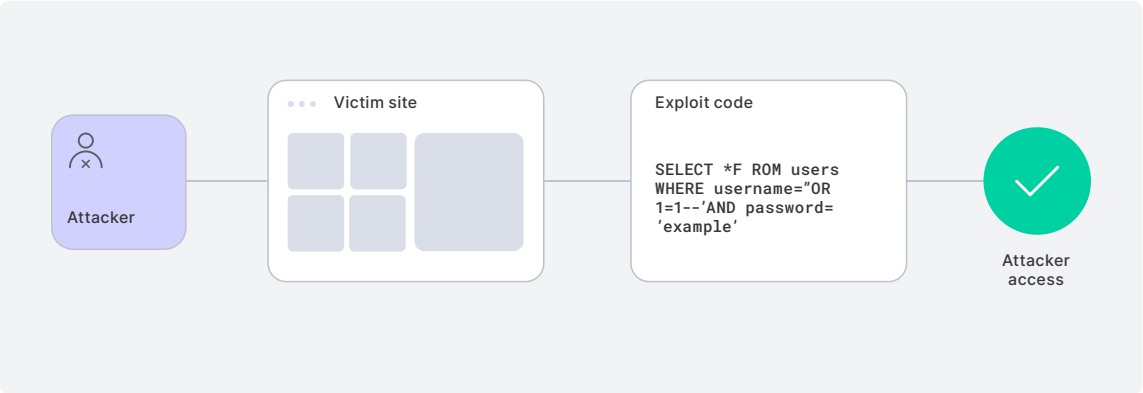


Injection

Injection attacks insert code into a field, like a username, to exploit poorly implemented systems that fail to sanitize inputs. For instance, the code might instruct the backend to ignore the password check and automatically log the attacker into the first account in the database of users, which is often an administrative account.

Once an attacker has administrative access, a wide range of intrusion actions become available.

Figure 15: Anatomy of an injection attack



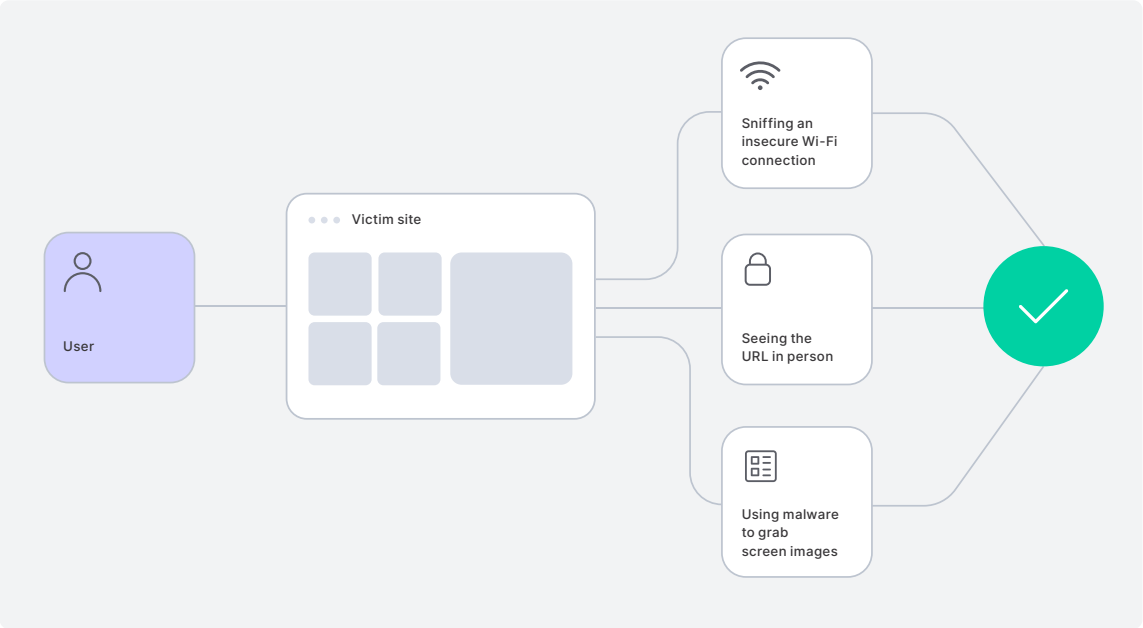
Session ID URL Rewriting

Like session hijacking, session ID URL rewriting is an attack that provides a threat actor with account access; in this case, the attacker steals the session URL — which can be achieved in a number of ways, including:

- Sniffing an insecure Wi-Fi connection
- Seeing the URL in person (e.g., looking over someone's shoulder)
- Using spyware/malware to grab screen images

As with session hijacking, the attacker maintains account access for the duration of the session.

Figure 16: Anatomy of a session ID URL rewriting attack



Part 2: Regional Spotlights

While understanding attack patterns — both the techniques and the target verticals — is important, so too is recognizing that the volume and type of threats facing CIAM systems can vary by the application and service provider's geographic location.

Figures 17 through 26 show the daily count of different login events observed by the Auth0 platform in different countries and regions for the first 90 days of 2022.

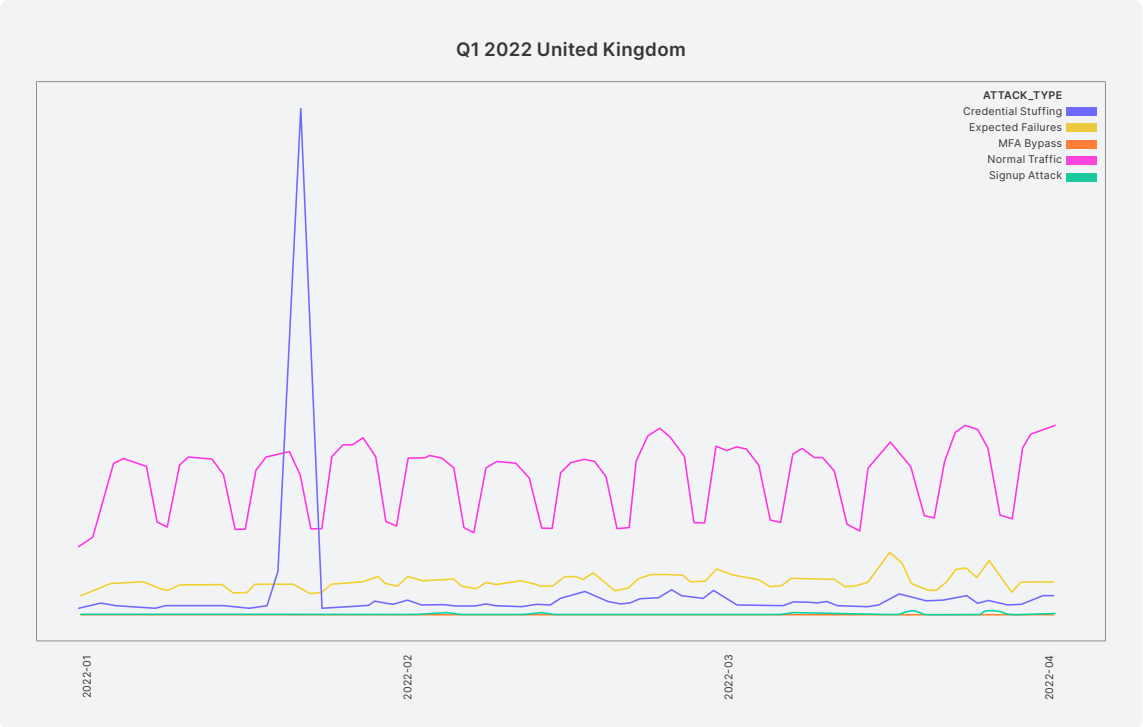
Inspecting each graph individually shows the relative volume of different identity attacks within a particular locale, while examining them in aggregate demonstrates the considerable geographic variation.

Europe

The United Kingdom (Figure X) is a good place to start our tour, as its traffic profile shows the weekly ebb and flow of login events indicative of normal behavior — and also one large-scale credential stuffing attack in the middle January.

Outside of this incident, normal traffic accounts for the large majority of login events, and the volume attributable to genuine failures (e.g., user errors) exceeds that of attacks.

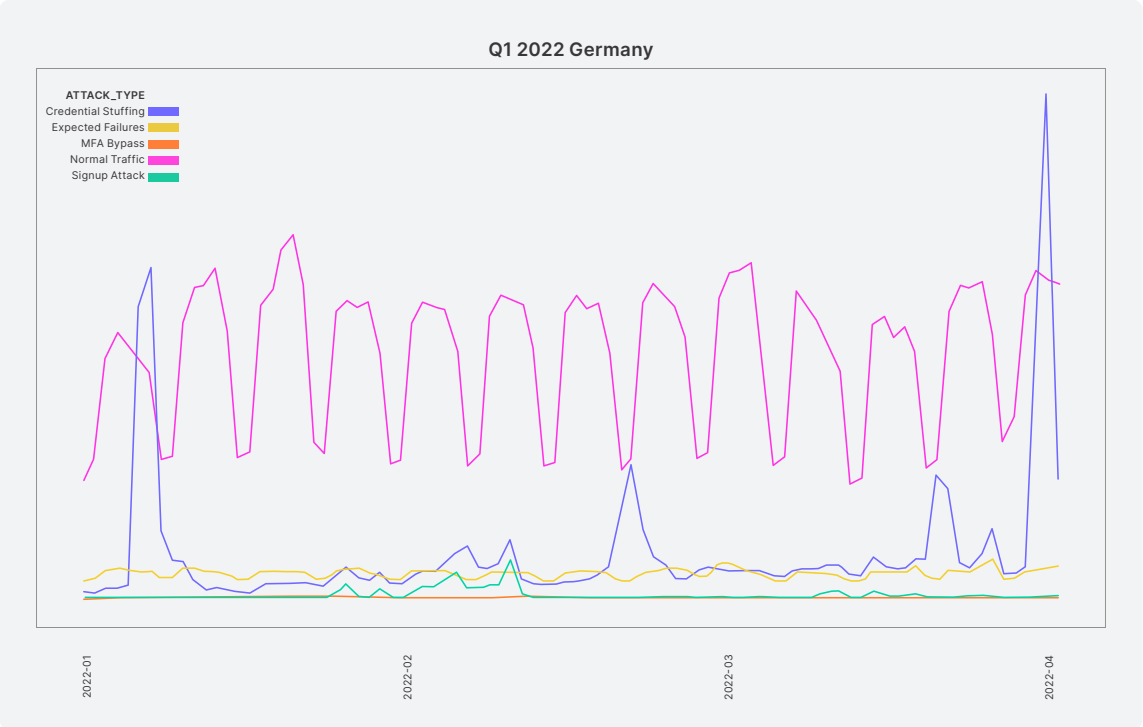
Figure 17: Identity traffic attribution for the United Kingdom during the first 90 days of 2022



Looking now to continental Europe, Germany's traffic attribution (Figure 18) is quite similar to the UK's: normal traffic accounts for most events and we see evidence of ongoing, low-level credential stuffing punctuated by larger-scale attacks.

One notable difference is that the 'background' volume of attack traffic is a bit higher relative to expected failures than we observed in the UK.

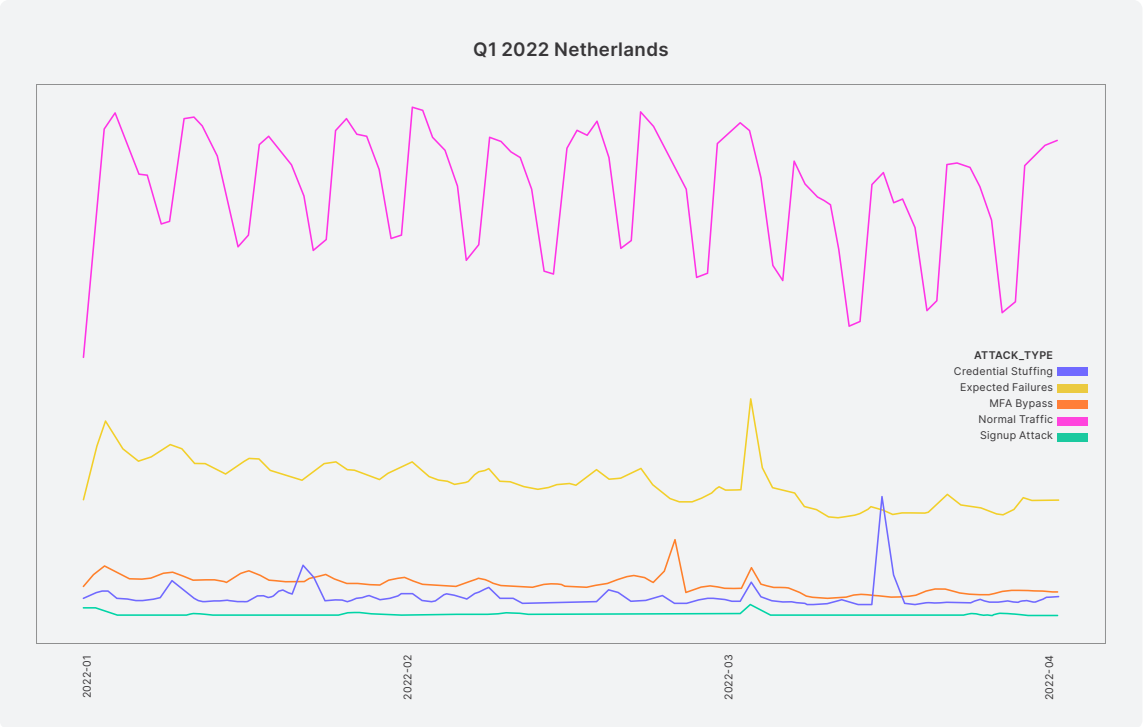
Figure 18: Identity traffic attribution for Germany during the first 90 days of 2022



Crossing the border into the Netherlands (Figure 19), we again see that normal traffic accounts for the majority of login events (70%); however, we don't see any large-scale attacks within this observation window.

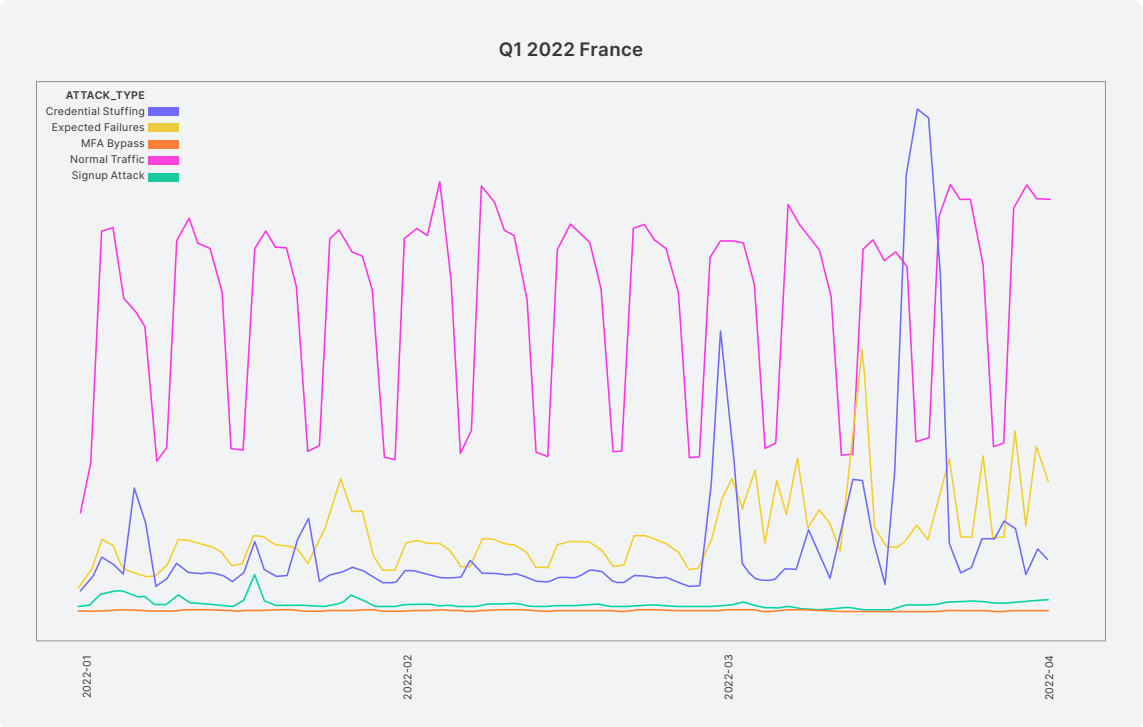
In fact, the share of login events attributable to malicious activity is the lowest of the geographies examined so far: credential stuffing attacks account for only (3%) of login events, trailing even MFA bypass attacks (5%).

Figure 19: Identity traffic attribution for the Netherlands during the first 90 days of 2022



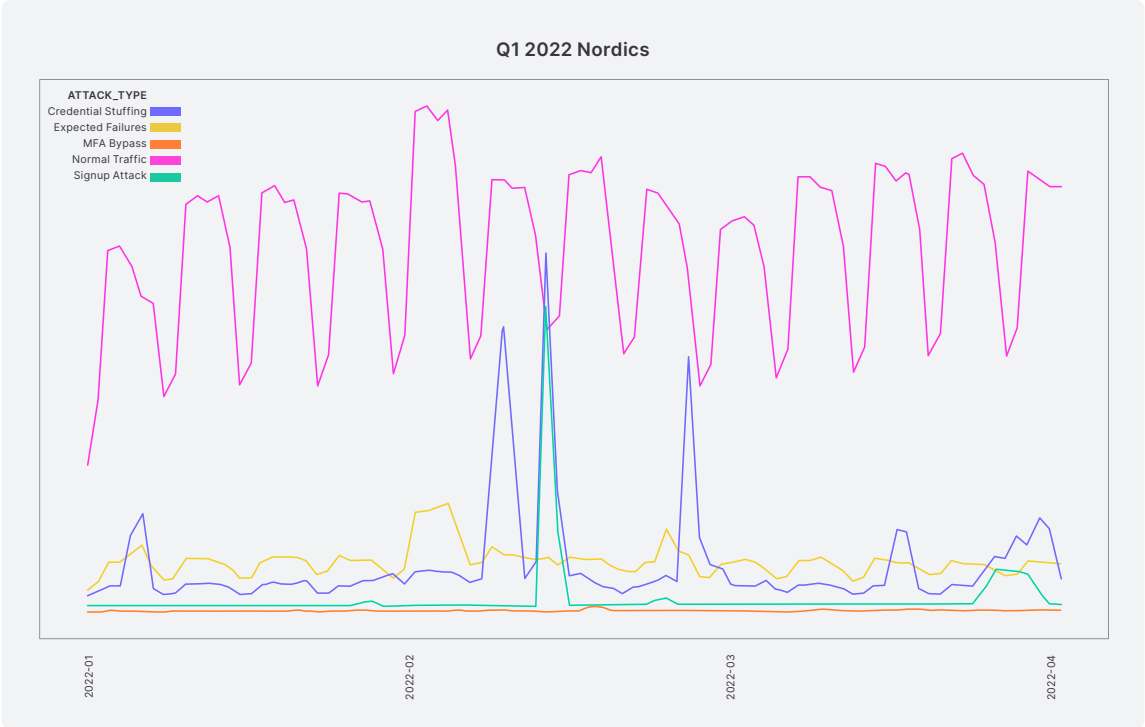
Continuing our westward journey into France reveals a profile (Figure 20) similar to Germany's: normal traffic represents the majority of login events, while credential stuffing is an ever-present threat, and there are a few signup attacks that rise up beyond the background level.

Figure 20: Identity traffic attribution for France during the first 90 days of 2022



For the most part, the Nordic nations (Figure 21) in aggregate exhibit a similar traffic profile as their continental peers. However, right in the middle of the observation window we can see a large-scale signup attack that aligns with a large-scale credential stuffing attack.

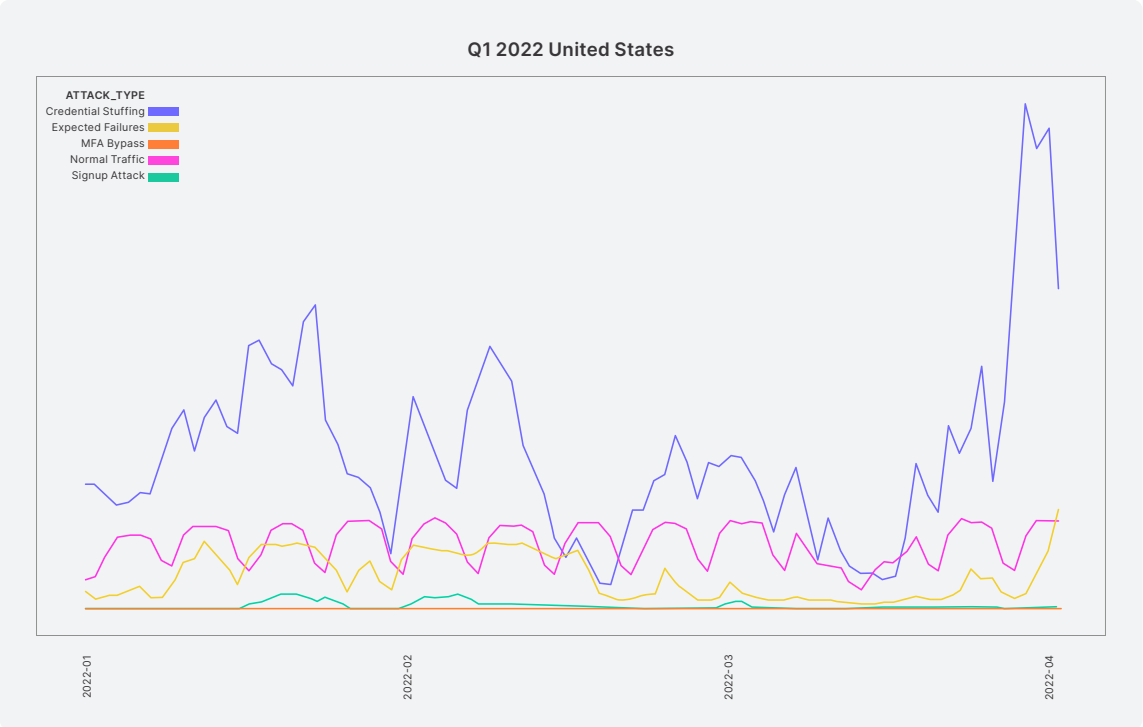
Figure 21: Identity traffic attribution for the Nordics during the first 90 days of 2022



The Americas

The United States (Figure 22) presents a stark contrast to what we observed in Europe. During the same observation window, credential stuffing accounts for the largest proportion of login events — 61% overall and soaring to 85% of login events during the attack at the far right side of the graph — vastly exceeding signup attacks (1.3%), MFA bypass attacks (0.16%), normal traffic (38%), and genuine user failures.

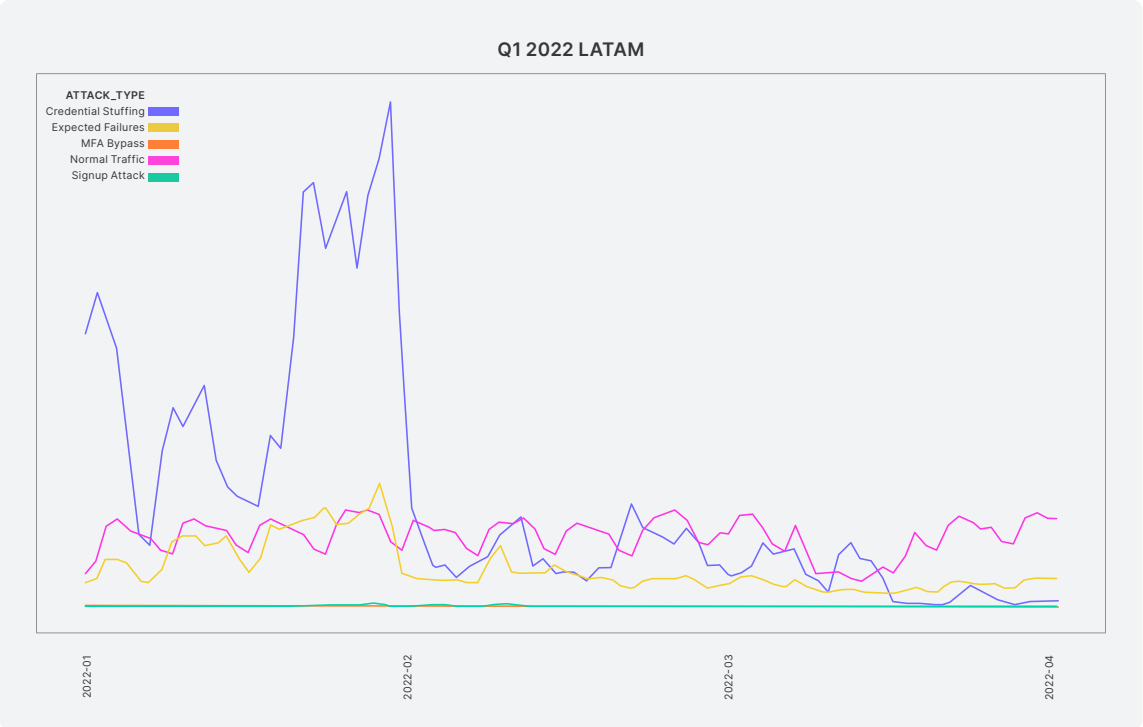
Figure 22: Identity traffic attribution for the United States during the first 90 days of 2022



For the first month of the observation window, the traffic profile for Latin America (Figure 23) is barely distinguishable from that of the United States; then, the large-scale credential stuffing adopts a new steady state just below that of normal traffic.

While the reasons for this abrupt shift aren't known, this graph illustrates just how suddenly attack traffic can change.

Figure 23: Identity traffic attribution for Latin America during the first 90 days of 2022

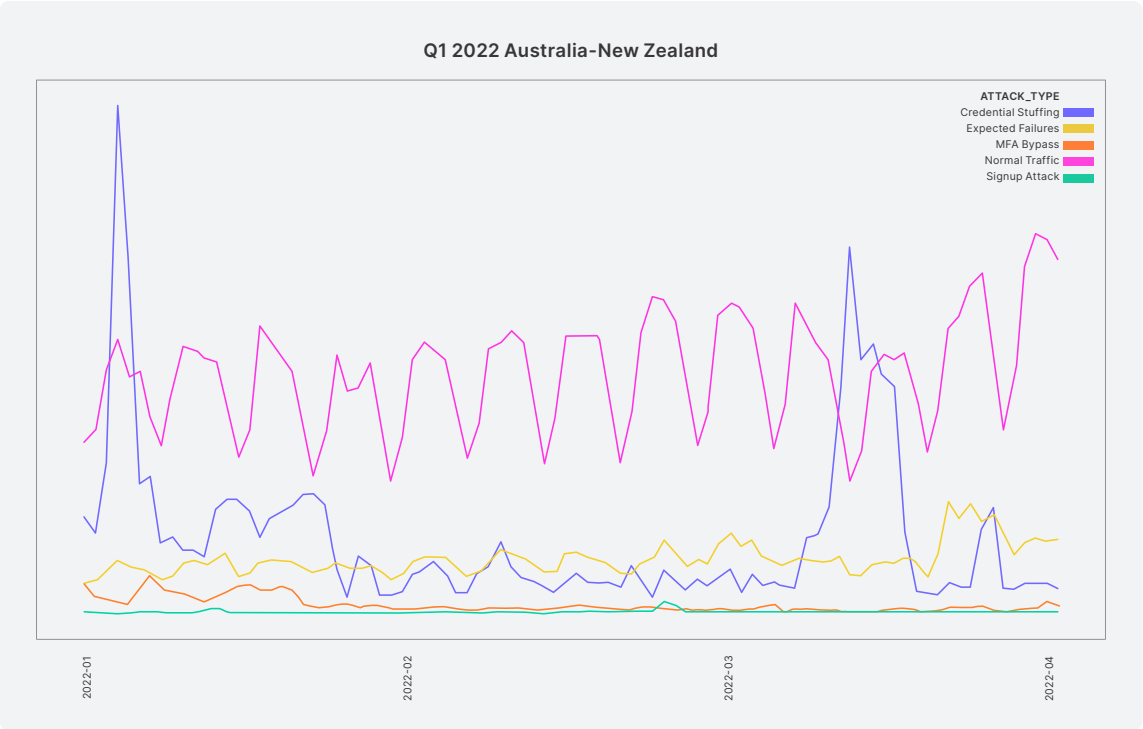


Asia-Pacific

In Australia and New Zealand (Figure 24), normal traffic represents the majority of login events (63%), and only during large attacks does credential stuffing overtake legitimate traffic.

In this region, MFA bypass attacks are responsible for more events than signup attacks — a reversal of the situation typically observed elsewhere.

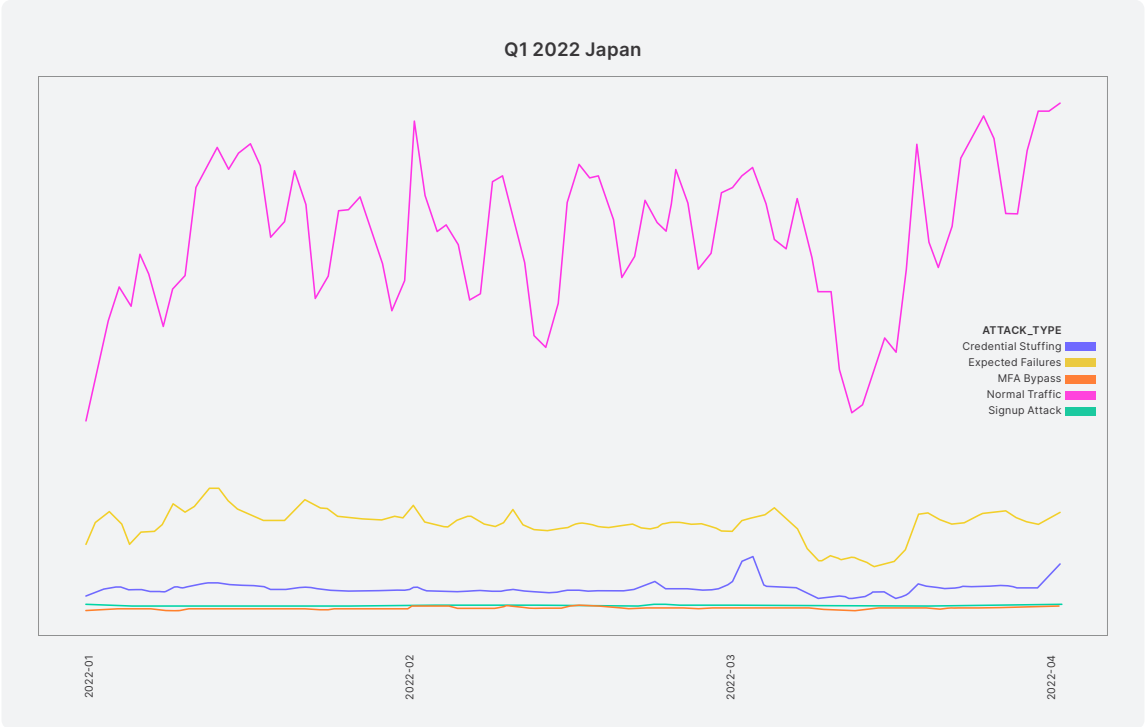
Figure 24: Identity traffic attribution for Australia and New Zealand during the first 90 days of 2022



Japan's traffic profile (Figure 25) is about as innocuous as one could hope to observe, with normal traffic accounting for the vast majority of events and outnumbering expected failures by a strong ratio, and with malicious events barely registering.

It's worth noting that of all the profiles presented in this section, Japan's seems to most closely resemble the Netherlands', further driving home that while geographic neighbors may have significant differences, regions that are far apart may exhibit strong similarities — but, most importantly, that the only way to truly know what's happening in a particular region is to observe it directly.

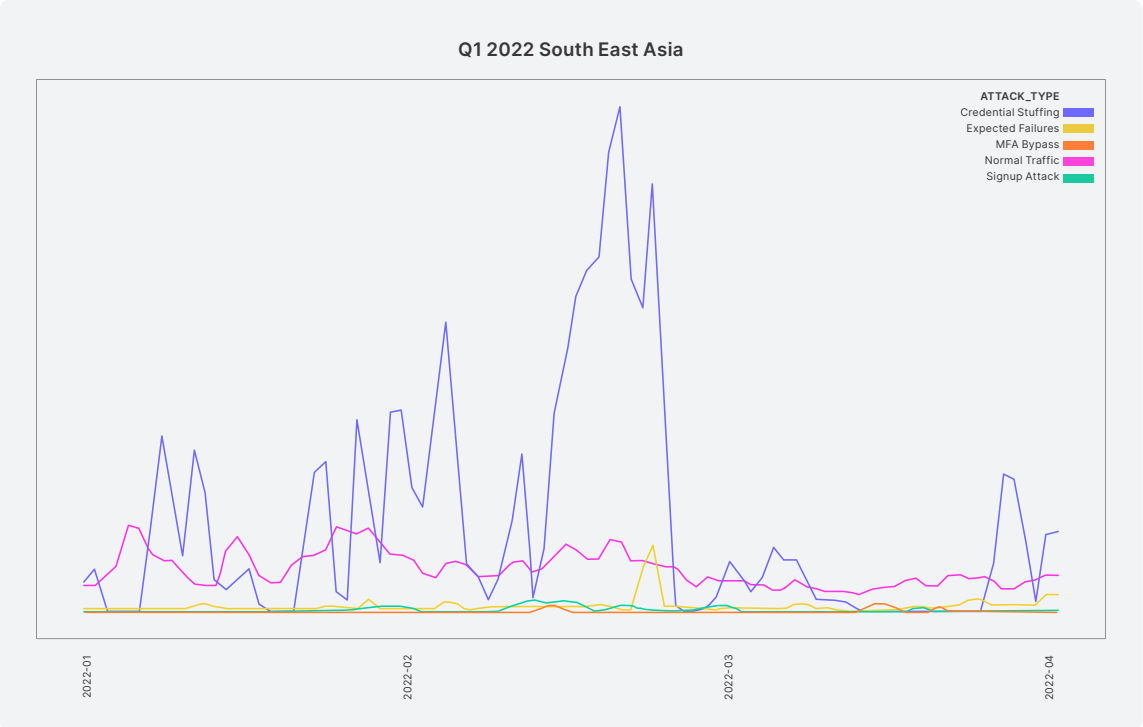
Figure 25: Identity traffic attribution for Japan during the first 90 days of 2022



The profile for South-East Asia (Figure 26) is reminiscent of what we saw for North America: buoyed by several large-scale attacks, credential stuffing accounts for the majority of identity events.

What appears to be a single large-scale credential stuffing attack in the middle of the observation window is actually a combination of separate attacks against targets in three industries (SaaS/Technology, Travel, and Financial Services). We can say with high confidence that the attacks are distinct, because their characteristics (e.g., source IPs, user agents, behaviors, etc.) differ significantly.

Figure 26: Identity traffic attribution for South-East Asia during the first 90 days of 2022



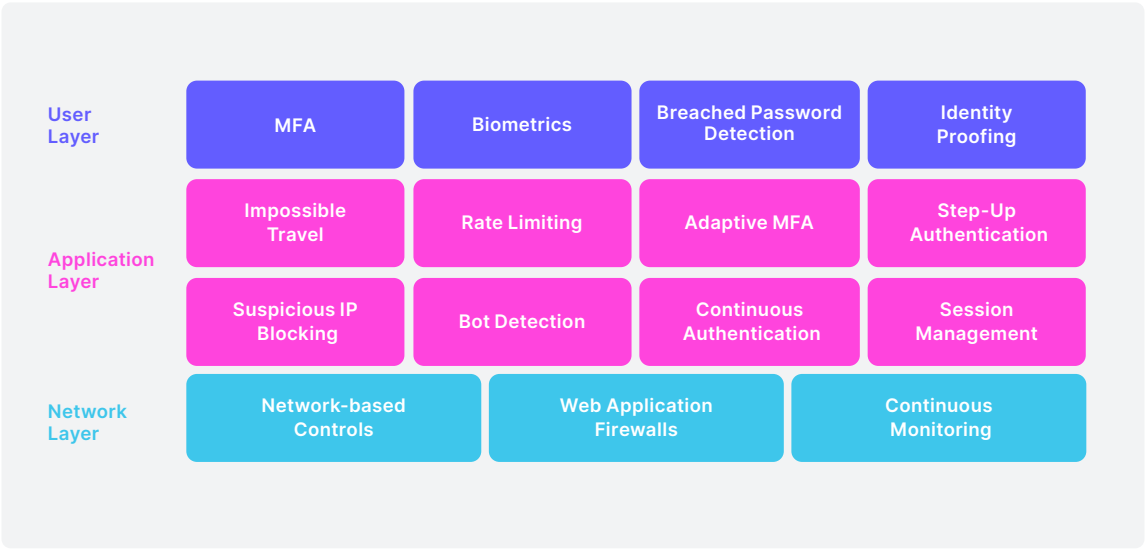
Part 3: Managing CIAM Threats

As adversaries focus greater attention on attacking identity systems and evolve their tactics, techniques, and procedures (TTPs), it is essential for application and service providers:

- To implement defense-in-depth tools that work in combination across the user, application, and network layers (Figure 27);
- To continually monitor their applications for signs of attacks and changes in TTPs; and
- To make adjustments (e.g., tune parameters, tighten restrictions, introduce new tools, etc.) as needed.

An agile, secure-by-design CIAM solution permits a considerable amount of flexibility that allows organizations to strike an optimal balance between security and user convenience — and even to customize this balance depending upon your risk appetite, user experience requirements, and implementation.

Figure 27: Securing CIAM requires a defense-in-depth strategy employing many complementary tools and techniques



User-layer defenses

User-layer defenses are 'implemented' by users to protect their own identity on an individual basis (e.g., MFA, WebAuthn) or that involve the user in some way (e.g., prompting the user to change their password, using identity proofing).

In general, application and service providers should ensure that MFA is used whenever possible and that specific measures be in place to identify accounts relying on credentials that are known to have been breached; in some cases, identity proofing is an additional necessity.

Multi-factor authentication

Having to overcome MFA drastically increases the time and effort needed for the attacker to compromise the account, which makes it infeasible to do at scale.

However, it's essential that the solution is implemented properly and uses strong secondary factors.

As noted earlier, technologies that are effective in consumer applications must balance security and usability and one way to assess the quality of user experience is by examining two measurements:

- The passing rate of an authentication challenge: the higher the passing rates, the better the user experience.
- The time to complete an authentication challenge: the shorter the time to complete, the better the user experience.

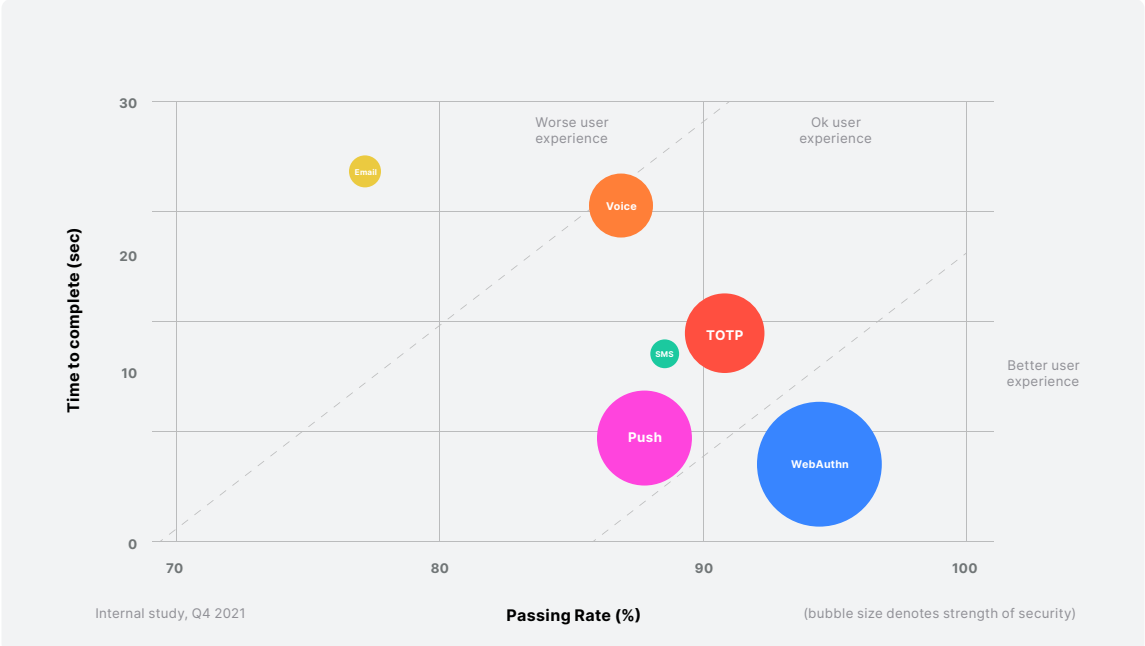
Combining these two measures and comparing across different authentication challenges shows that the user experience varies significantly. Visually examining Figure 28 reveals that:

- Voice and email authentication provide a poor user experience: passing rates are comparatively low and the time to pass is comparatively high.
- Push via a proprietary application (Push), pushing a one-time password (TOTP), and using SMS as an MFA channel deliver a middle-of-the-pack experience.
- Leveraging device biometrics (WebAuthn) delivers the best user experience — combining high passing rates and low time to complete the challenge.

Interestingly — and importantly — we can also see a high degree of correlation between those authentication challenges that deliver a convenient user experience and those that provide the best security.

In fact, biometrics like WebAuthn are a great example of how CIAM systems can simultaneously deliver a convenient, private, and secure experience.

Figure 28: Securing CIAM requires a defense-in-depth strategy employing many complementary tools and techniques



WebAuthn

MFA methods based on WebAuthn-enabled device biometrics (e.g., Apple Face ID, Apple Touch ID, Windows Hello) or WebAuthn-enabled security keys (e.g., YubiKey, Feitian, Titan) offer a powerful combination of strength and low user friction and represent a big step forward for security and user experience.

Implemented via a WC3 Web API, WebAuthn allows browsers to authenticate using a public/private key pair generated for each user/device/website, instead of shared secrets. Importantly, because it guarantees that credentials are only valid for the websites where users actually registered, the method is not vulnerable to phishing.

WebAuthn is relatively new, so adoption remains fairly limited at this time; nevertheless, WebAuthn holds tremendous appeal for both users and application providers, so enrollment is expected to grow substantially

Improving password management

In addition to implementing breached password detection, some simple — but effective — ways to enhance identity security are to:

- Require strong passwords
- Prevent users from repeating their passwords
- Compare potential passwords against a dictionary to prevent use of common passwords
- Implement a good password reset process

Password reset is a necessity for any app. But building a good password reset process is more than asking security questions. If your password reset process makes life harder for your customers, you'll be giving them a reason to stop using your service.

Good password reset processes do two things:

1. They minimize friction for the customer: It shouldn't take your customer more than a minute to reset their password, and the process should only require information customers are comfortable entering, like email addresses
2. They make sure the customer's information is secure: Providing safeguards against things like multiple failed logins and only sending information via secure channels

Email is most commonly used for password reset because it satisfies both these criteria. It minimizes friction as typing in an email address is quick and easy for a customer, and it will protect their information as only the customer should have access to their inbox.

A single misstep in password reset can ruin your customer's entire experience with your product. These mistakes often come in the form of:

- **Security questions:** Static information is easy to obtain — where you went to school, your mother's maiden name, even your pet's name, are probably available somewhere on the internet, making them available to attackers
- **Passwords in plaintext:** Instead of resetting the password, some sites send the original password back to the customer, which is a massive vulnerability — for a password to be sent in plaintext, it must be stored in plaintext, which means that the chances of attack are increased

- **Error messages:** If an application says whether or not an email address is registered, an attacker could potentially know if a customer has an account — this gives them one more piece of information to use against your customer
- **Requiring unnecessary information:** Security must be balanced with usability — asking customers for a photo ID is a safe practice, but its overall effect on the customer experience is a negative one

Breached password detection

An unfortunate — but nevertheless very real — aspect of today's threat environment is that entire marketplaces exist to aid adversaries in their actions. For example, threat actors can easily purchase breached credentials and employ them for credential stuffing and account takeovers:

- 58% of all Auth0 customer applications have experienced at least one attack using breached/leaked credentials
- 25% of all Auth0 customer applications have experienced more than one such attack

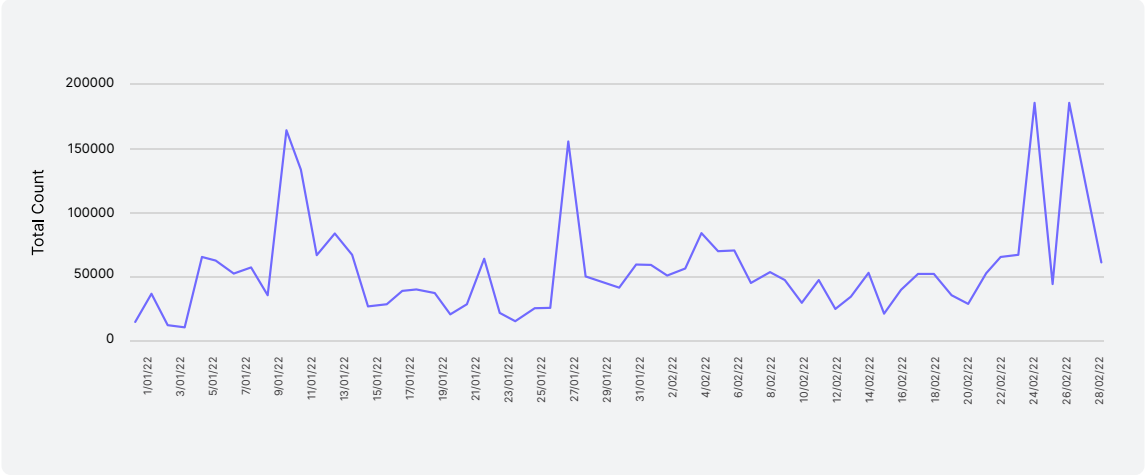
Figure 29 shows the volume of reused credentials observed by the Auth0 identity platform each day. The 'baseline' level of approximately 50,000 incidents per day is primarily attributable to password reuse on the part of users, with lower-volume credential stuffing playing a secondary role, while the spikes are indicative of larger-volume attacks employing breached credentials.

The risks caused by breached credentials can be somewhat managed by leveraging these same credential lists **to detect when users are employing a password that has appeared in a breach**. Upon detection, an application provider can warn the user and encourage or require some mitigating action on their part (e.g., change the password, implement MFA).

Fortunately, dedicated password managers and capabilities integrated into web browsers and operating systems are making it easier for users to create, safely store, and easily use longer and more complex passwords, thereby addressing some of the fundamental reasons why users choose and reuse weak passwords; plus, these same solutions often alert users when their credentials appear in leaks, increasing awareness of the risks.

Hopefully, the utility of breached passwords and the threat posed by them will decline as a result of these efforts.

Figure 29: Password reuse is largely responsible for a 'baseline' of breached passwords, while deliberate attacks account for observation spikes



Using social identities to combat password reuse

Social login provides single sign-on for end users. Using existing login information from a social network provider like Facebook, Twitter, or Google, the user can sign into a third-party website instead of creating a new account specifically for that website. This convenience simplifies registrations and logins for end users and enhances security because a user is more likely to recognize the importance of protecting — and to take the extra effort to protect — their critical social accounts.

Application providers enjoy benefits, too, including:

- **Increased registrations:** Many users prefer reusing an existing account over creating another new one
- **Verified email:** The social network provider is in charge of verifying the user's email. If the provider shares this information, then you will get a real email address rather than the fake addresses often used to register in web applications. Social providers will also handle the password recovery process.
- **Greater personalization and customization possibilities:** Social network providers can give you additional information users have consented to share, such as location, interests, birthday, and more, which you can use to enhance your services
- **One-click return experience:** After users register in your application using Social Login, their return experience will be very simple, as they will probably be logged into the social network, and just one click will be enough to login to your application.

Identity proofing

One of the most common misconceptions in CIAM is that authentication and identity proofing are equivalent, but while authentication (e.g., logging in with a username and password) shows that a user has the credentials that correspond to a particular account, it doesn't prove that the user is who they say they are — **that's where identity proofing comes in**.

Identity proofing uses additional verifications to create a high degree of confidence that your users are who they claim to be, in an effort to eliminate fraudulent signups and the consequences that come with them.

Within the CIAM context, it's important that identity proofing solutions scale, because CIAM typically demands real-time workflows to accommodate the spikes associated with seasonal variation and successful promotional programs, and in recent years, **a number of automated identity proofing techniques** have been developed to meet the demands of consumer businesses.

- Knowledge-based authentication (KBA), which leverages something a user — and, ideally, only that user — knows
- Document scanning and cross-validation, which uses a trusted photo ID — for example, a passport or driver's license — to verify that a user's claimed identity matches their actual identity
- Phone carrier verification, which takes advantage of the fact that the user's identity was already proven when they signed up for a phone service

Authentication after passwords

Traditional authentication is a digital barrier that suffers from many well-known flaws:

- Most login and account creation flows put too much burden and friction on the end user.
- Today's most widely adopted methods are far too easy for attackers to exploit.
- Traditional systems are unintelligent — as a result, they treat legitimate users and attackers the same way.

Because unnecessary friction in account creation and login is now recognized as a major deterrent to customer acquisition, conversion, and brand loyalty, in the coming years traditional authentication systems will be replaced by **passwordless** and — ultimately — loginless systems that simultaneously deliver convenient user experiences while preserving privacy and enhancing security.

While biometric authentication using WebAuthn is the shining example of passwordless, it is not alone: other methods also offer more convenience and stronger security than passwords, with fewer device dependencies than leading-edge biometrics.

Learn more about this bright future, including what you can do today, in **Authentication After Passwords: Maximizing conversions (and enhancing security) in the age of convenience**

Application-layer defenses

Application-layer defenses help to protect identity by providing security controls implemented across the application (as opposed to at the individual user level) intended to protect the application itself.

These defenses exist on a spectrum from tactical to strategic, and are most effective when used in combination and when customized to specific needs.

For example, application builders can combat fraudulent registrations by employing a number of techniques to tailor the level of authentication friction to the potential rewards of account creation, including:

- Using rate limiting (throttling) to counter brute force attacks by imposing restrictions on the rate at which a particular client can access the login interface: when a client exceeds a prescribed threshold, they may be required to complete a CAPTCHA, or may be restricted from accessing the login interface until a ‘cooling off’ or ‘penalty’ period has passed
- Applying pre-signup rules and actions to further reduce the chances that a new user is illegitimate
- Using identity proofing when risk is perceived to be particularly high

Impossible travel

Impossible travel detection flags incidents when a user attempts to sign in from a geolocation that would be impossible to reach within the time that has passed since the previous successful login — and therefore indicates a possible attack.

A positive detection can be incorporated into risk scores and step-up authentication workflows.

Rate limiting

Rate limiting (throttling) is a useful tool for countering high-volume, brute-force attacks by imposing restrictions on the rate at which a particular client can access the login interface.

This technique can be used in conjunction with others; for example, when a client exceeds a prescribed threshold, they may be required to complete a CAPTCHA, or may be restricted from accessing the login interface until a 'cooling off' or 'penalty' period has passed.

Suspicious IP blocking

Blocking suspicious IPs from accessing Internet-facing services has been employed for decades and still has utility today — provided its limitations are recognized.

The approach is simple:

- Some factor is used to determine the if an IP address can be trusted
- Addresses that fall below a prescribed trust threshold are denied access to the application

The same general technique can be applied to phone numbers, email addresses (for example, some applications only allow users from paid email services to register), and other variables.

To facilitate such filtering, many organizations subscribe to cybersecurity threat intelligence (CTI), others maintain a proprietary list of reputations based upon their own direct observations, and others combine these approaches.

One advantage of using a CIAM provider (as opposed to building your own identity solution) is that the vendor has massive visibility across hundreds or thousands of application and service providers, creating network effects that benefit everyone. For example, Auth0 observes an average of nearly 500,000 abusive IP addresses every week, and an IP observed attacking one client can be propagated within the platform to enhance the safeguards protecting every other client.

Using geolocation as a trust factor

Integrating the geolocation of an IP address into risk scoring algorithms is useful, but application providers should not assume that 'local' origins are inherently trustworthy.

Figure 30 is a co-occurrence graph that maps the top 25% of abusive IP geolocations (Y-axis) against the target country (X-axis). The brighter a cell, the higher the number of attacks originating from IP addresses within the Y-axis country against the X-axis country.

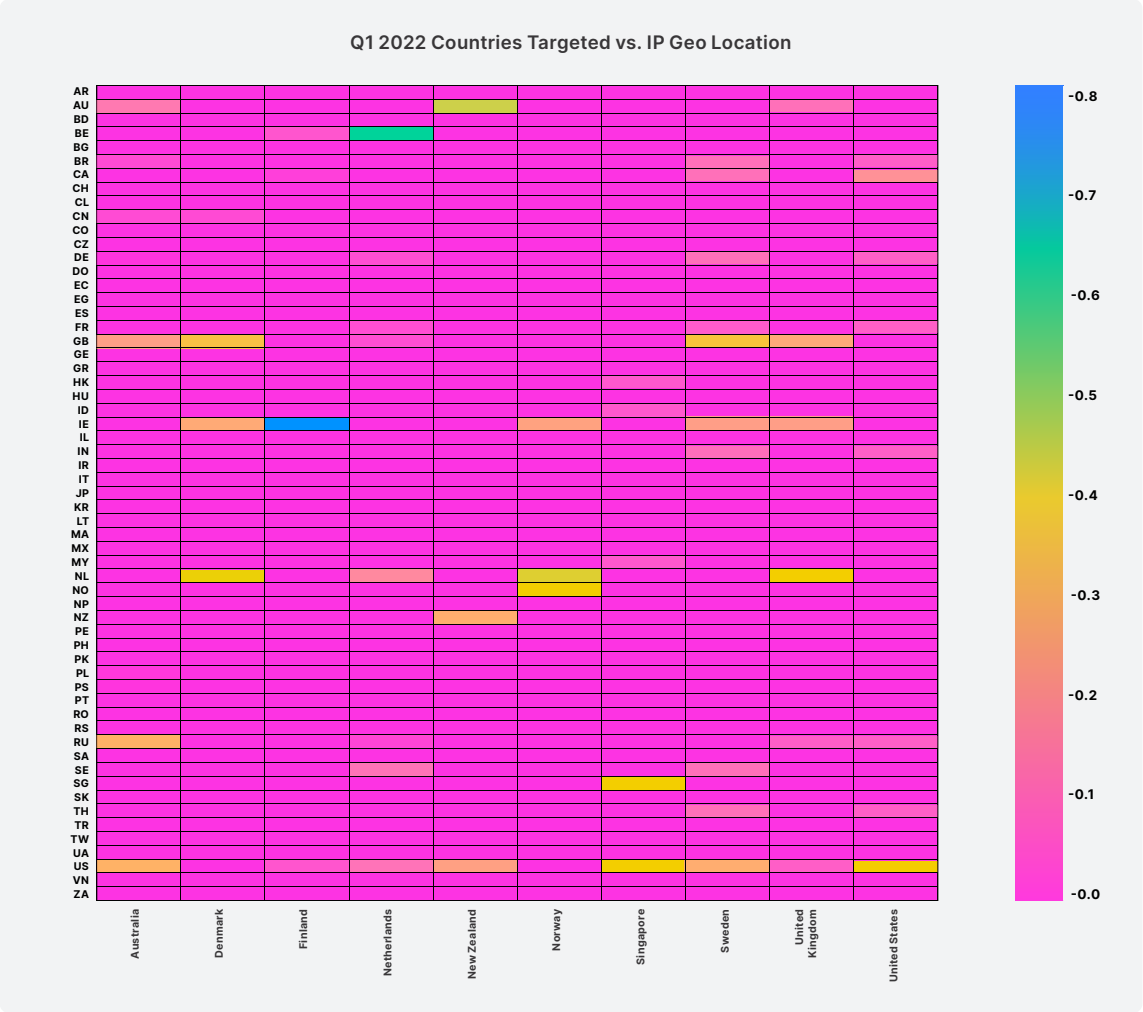
Careful examination reveals two important insights:

- Many attacks appear to originate from within countries with generally good reputations (e.g., the United States, the Netherlands, Great Britain, and Ireland).
- A number of countries are being targeted from within (e.g., US v United States, SG v Singapore, NZ v New Zealand.

These observations strongly suggest that threat actors are taking steps to ensure their attacks appear to originate from locations close to the target.

In fact, playbooks readily available online often show would-be attackers how to use VPNs, SOCKSv6 proxies, or other techniques (and convenient services) to manipulate IP addresses to evade region-specific filters and impossible travel detections.

Figure 30: Threat actors are working to evade geolocation-based detection mechanisms



Bot detection

Bot traffic plagues identity flows at all points of the user journey. But it also has a hidden cost.

Considering that in the first 90 days we saw tens of billions of bot-initiated login requests, this equates to potentially millions of dollars in compute costs just to accommodate that bogus traffic.

By correlating a variety of data sources, it's possible to create friction for scripted attacks like credential stuffing and password spraying by detecting when a request is likely to be coming from a bot.

The request can then be blocked or ignored, as allowing a threat actor to enter credentials into a login interface runs the risk of providing valuable intelligence — especially if you use more than a single generic error message.

A bot detection algorithm can incorporate past events associated with an IP address, recent login history, IP reputation data, and other factors to generate a confidence score; based upon this score, you can show the login screen or first challenge the visitor to complete a CAPTCHA.

In Auth0's direct experience, such a defensive layer can reduce the success rate of a credential stuffing attack by as much as 85%.

Adaptive MFA and Step-Up Authentication

Achieving a balance between security and usability is vital for creating a positive user experience. Two closely related ways for fine tuning that balance are:

- Adaptive (or contextual) MFA; and
- Step-up authentication.

Traditional MFA as outlined earlier is incredibly effective in preventing attacks, but it comes with a usability cost because it requires additional steps that a user must complete in order to continue with the interaction. Adaptive MFA is a technique that only engages MFA when a user interaction is deemed risky based on behavioral data (e.g., an unknown device, impossible travel, IP reputation, risk scoring, etc.).

By reserving MFA for risky scenarios, adaptive MFA maintains security while preserving the frictionless experience for the majority of users.

Step-up authentication also empowers application providers to strike a balance between security and friction, in this case by adapting identity requests to the importance of the resource and the risk level if it were to be exposed. It ensures users (or whomever might be posing as a user) can access some resources with one set of credentials but will prompt them for more credentials (e.g., MFA) when they request access to sensitive resources.

The risk with step-up authentication is in the implementation — **effective implementations** require careful planning about to whom you grant access and whom you ask to step up.

Continuous authentication

Just because a user passed an authentication challenge initially is no reason to necessarily provide long-lived access.

By continuously monitoring signals (e.g., the user's location, device, apps, consumption patterns, time of day, input behavior, etc.), the authentication system simply checks, whenever needed, to see if the trust is still sufficiently high to allow the user ongoing access.

This "continuous authentication" is extraordinarily powerful, as it enhances both security and the user experience — and the trust that it delivers extends far beyond anything a password by itself can provide.

Session management

Here are three ways to improve session security to guard against session hijacking and session ID URL rewriting attacks:

- Avoid putting session IDs in the URL
- Use a server-side, secure session manager that generates a new session ID after login
- Securely store session IDs and invalidate them after logout

Network-layer defenses

Despite the well-documented dissolution of the traditional 'hard' perimeter, defenses implemented at the network layer can still make meaningful contributions to application security — again, provided the limitations are recognized.

Network-based controls

Intrusion detection systems (IDS), Zero Trust Network Access (ZTNA), and allow/deny lists still have their place in protecting your application and its ability to deliver service.

Web application firewalls

Web application firewalls (WAFs) can be very useful for filtering standard types of attack against your application, particularly when you're able to tune the WAF to the exact needs of, and abuses against, your application.

However, achieving this tailored configuration can be challenging and time consuming, and whether or not doing so is worthwhile depends upon your risk tolerance and appetite.

It should also be noted that while WAFs can help to mitigate some types of bot-based attacks, many botnet operators continuously modify the behavior of bots to avoid these types of security controls — which is why dedicated bot detection is a modern necessity even when WAFs are present.

Continuous monitoring

Finally, consider continuous monitoring. For example, watch for changes to the baseline usage of your application; if traffic volumes suddenly increase and no benign cause is known, then it could be a sign of an attack and you may need to tune your layers of defenses accordingly.

Conclusions and Recommendations

For customer-facing application and service providers, robust and resilient CIAM capabilities form the security perimeter and are essential to safeguard against fraudulent registrations and account takeovers — and the significant consequences caused by these abuses.

Stopping today's sophisticated credential stuffing attacks, signup attacks, MFA bypass attacks, and other identity threats and disrupting threat actor business models — while preserving an appropriate level of friction for legitimate users — is only possible by combining multiple security tools, operating at different layers, into a cohesive defensive posture.

In the context of CIAM, this layered approach corresponds to employing defensive measures before and throughout the authentication workflow at the user, application, and network layers.

Sourcing, integrating, configuring, and continuously monitoring, tuning, and orchestrating these tools on a solution-by-solution basis requires rare skills, consumes considerable operational attention, and pulls valuable resources that are better directed towards advancing a company's core competencies.

For these reasons and others, a best-of-breed CIAM solution with an agile, secure-by-design, defense-in-depth architecture is a much more effective approach to achieving identity security compared to building and maintaining an identity stack in house.

In either approach, the challenge for application builders is to develop and implement security measures that strike an appropriate balance of increasing friction for attackers while respecting the user experience. Whether you are developing your own in-house solutions, or relying on an identity-as-a-service provider, here are some fundamental recommendations:

- **Implement and encourage MFA:** MFA is one of the most effective ways to disrupt attacks — implement multiple methods with strong secondary factors and encourage user adoption. Embrace WebAuthn and enable it on supported devices.
- **Use the same failure messages:** Detailed failure messages can assist threat actors by providing information about users that exist in the system. Keep attackers in the dark by providing generic failure messages.
- **Limit failed login attempts:** Brute force, credential stuffing, and password spraying often trigger many failures for each successful login. Use this behavior to detect attacks and trigger countermeasures.
- **Implement secure session management:** Use a server-side, secure session manager that generates a new session ID after login. Don't put session IDs in the URL, and do ensure they are securely stored and invalidated after logout.
- **Don't ship with default credentials:** Default admin credentials are a major attack vector because many users leave them unchanged, leaving systems vulnerable to dictionary attacks.
- **Enforce strong passwords:** Many brute force attacks rely on weak or common passwords. Enforce password length, complexity, and rotation based on NIST recommendations or other evidence-based policies.
- **Monitor for breached password use:** Many users reuse the same or similar passwords across multiple sites, so a breach in one service can threaten many others. Force users to change breached credentials.
- **Don't store plain-text passwords:** If your password database is truly illegible, then it has no value to hackers. Encryption makes your organization a much less appealing target, but the implementation must be sound.

Learn more about identity management with Auth0

Identity is vital to enabling online applications and will become even more important as the zero trust paradigm gains wider adoption. Identity is also difficult — even seasoned pros find creating effective and efficient implementations to be challenging. Auth0 takes on the burden of identity and access management, so you can focus effort and energy on delivering core business value.

Disclaimer

This document and any recommendations about your security practices is not legal, security, or business advice. This document is intended for general informational purposes only and may not reflect the most current security and legal developments nor all relevant security or legal issues. You are responsible for obtaining legal, security, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein. Okta is not liable to you for any loss or damages that may result from your implementation of the recommendations in this document.

Afterword: Actions for CISOs

After reviewing the insights gathered by Auth0 Security Architect Kim Berry and our data team, meeting with customers and prospects, and speaking with other CISOs, these are the actions I'm hoping to see us all take:

- **Make identity security a board-level issue.**
  It's hard to get the board to fund what they don't understand, which is why we created this one-pager that you can share with your CTO, COO, CEO, and other executive leaders and board members.
- **Revisit existing controls and implement new ones.**
  Every organization should determine its own risk tolerance and must recognize that attackers are always evolving their TTPs to seize opportunities and evade defenses. What was appropriate or what worked before may not be the best approach today.
- **Collectively work towards clear security industry standards that make sense to decision makers, but also to insurance companies.**
  Cyber insurance premiums have soared in the past 12 months, eating into the budgets we need for controls and for the talent to manage them. In the next year, I'll be working towards generating clearer methods for evaluating and mitigating risk and extending proven Zero Trust principles to the CIAM space.

At the end of the day, security is about protecting real people alongside protecting businesses and other organizations. As online or click-and-mortar interactions play larger roles in our lives, so too does the related data become a target — and the harder teams like mine need to work to ensure secure, private, and user-friendly experiences. The threat landscape is going to keep evolving, and it's our job to stay ahead of it.

— JAMEEKA GREEN AARON, CISO, CUSTOMER IDENTITY, OKTA

Auth0 is an easy-to-implement, adaptable and secure authentication and authorization platform. Built on a set of composable building blocks exposed through APIs and protocols, the Auth0 Identity Platform provides multiple solutions to address any identity use case without forcing a compromise between convenience, privacy or security.

Learn more at **auth0.com/identity-platform.**