Darwinium

Darwinium Account Security: Continuous Customer Journey Protection

Digital account security remains an unsolved problem. Businesses are currently relying on legacy solutions that were built to protect high-risk touchpoints - such as onboarding, login or payments - but are repeatedly breached by fraudsters targeting new vulnerabilities in the customer journey. The speed and efficacy of attacks have increased, facilitated by AI tooling and human click farms. Businesses are restricted by siloed systems, multiple disparate solutions, and privacy constraints that fraudsters bypass.

Key:

The icons/colours below are used throughout this document and correspond to the following:



Account Security Risk Type / Sub-type



Account Security Risk Type / Sub-type Methods



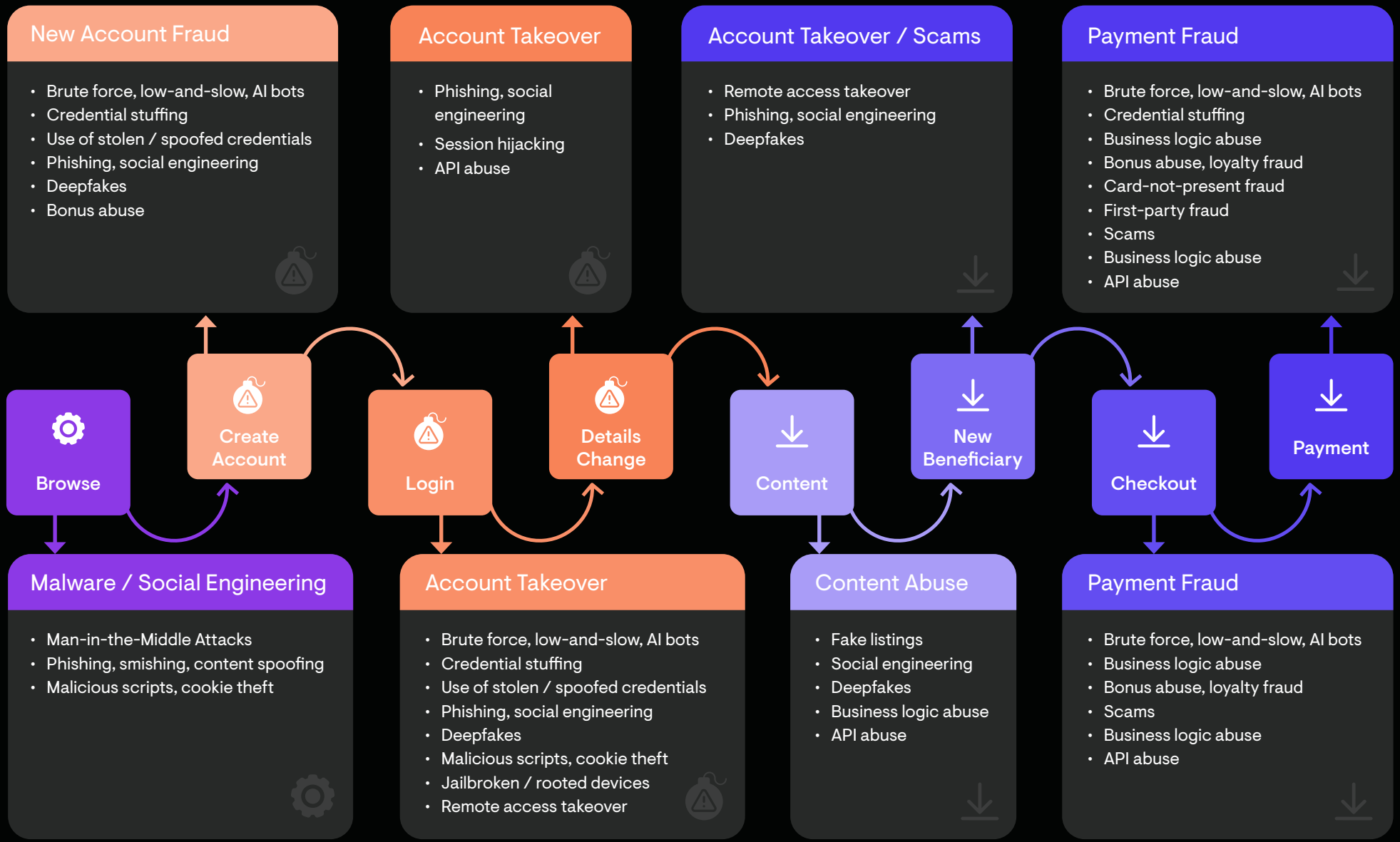
Downstream Harms

Glossary:

Click here to view the Glossary.

Persistent Threats Across the Customer Journey

Numerous, persistent threats exist across the entire account security customer journey, from pre-authentication behaviors, such as browsing and adding to cart, through new account creations, logins and content creation, to change of details, checkout, and payments:





Existing Solutions Lack the Combination of Visibility and Context of User Behavior

Security tools typically have good visibility of traffic behavior, but lack the context of user behavior to stop advanced account takeovers and scams.

Fraud solutions provide a greater depth of intelligence at key touchpoints, but typically lack holistic protection across the complete customer journey, creating siloed protection and a disparate view of customer data.

Why Darwinium?

Darwinium is a cyberfraud prevention platform that is solving the toughest challenges in account security by providing complete visibility of user behavior across every digital touchpoint.

Real-time analytics are combined with the ability to decision and act on intelligence immediately. This provides agility and control to protect end user accounts from complex bots, fraud, scams and abuse, and adapt to evolving threats as they happen.

The entire ecosystem is designed to maintain the privacy and security of end users, only ever using a truly anonymized version of encrypted data.

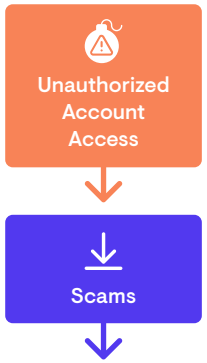
Darwinium can integrate on the perimeter edge using content delivery network (CDN) infrastructure, providing rich behavioral analytics, context and decision management capabilities across every digital interaction, and every customer journey. It goes beyond the point-in-time risk assessments of legacy fraud solutions, to building behavioral identification across complete digital journeys. Darwinium's flexible decision engine also allows businesses to make real time risk decisions, as well as conditionally integrate third-party solutions, with a series of plug and play integrations, or any preferred data source, via an API, to enhance risk decisions.

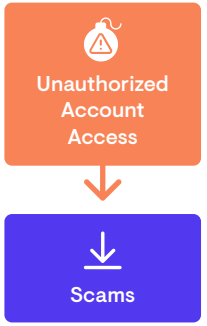
Account security covers an extensive set of challenges, from bot protection, onboarding and account takeover protection to payment security, loyalty and bonus protection, business logic abuse, scams and social engineering. Darwinium's cyberfraud prevention platform provides a complete solution to account security, with future-proofed capabilities designed to react to evolving threats as they happen, rather than retrospectively.

Darwinium for Account Security

Threat	Existing Solution Shortfalls	Darwinium Capability / Benefits	Darwinium Proof Points	Use Case
Advanced / Persistent Bot Attacks • Automated bot attacks are becoming more intelligent and human-like, facilitated by Large Language Models (LLMs) and machine learning, to make them less predictable and harder to detect – in the case of marketplaces, LLMs can generate infinite permutations of user-generated content such as listings. • Bots can be programmed to spend variable amounts of time on pages and navigate web pages in ways that closely mimic human behavior. Furthermore they can be programmed to operate within time-of-day constraints in order to circumvent detection. • Advanced bots can now solve CAPTCHAs using machine learning algorithms that recognize patterns in CAPTCHA images. • Bots can also adjust behavior based on context, such as changing language, tone, and interaction style according to the website they are interacting with. • Some bots can create detailed user profiles, storing cookies and session information to appear as returning users, which can fool detection systems that rely on session analysis. • Low-and-slow bots mimic customer traffic velocities and behaviors, bypassing rate control measures to infiltrate customer accounts. • Modern bots can even simulate human browsing habits, such as randomizing mouse movements, clicks, and typing patterns, which helps them blend in with legitimate users.	Current bot solutions are blunt instruments – making binary risk decisions based on limited information and lack the deep contextual intelligence to separate unusual human behavior from human-like bot behavior. Businesses lack the context of behaviors both upstream, from the edge, and downstream, from payment attempts, to inform accurate risk decisions. Current step-ups, such as Captchas solutions, are negatively impacting good customer traffic without stopping bot traffic. Many bots are more adept at solving CAPTCHA puzzles than humans are.	**Digital Signatures** • Detect and block bot behaviors using digital signatures for devices and behavioral biometrics. Identify unusual velocities, credential stuffing and proxies / emulators, even if they are tuned to bypass existing controls. • AI bots can be separated by intent to identify nefarious activity versus trusted, aggregator or customer behavior. **Behavioral Biometrics** • Detect automated behaviors indicative of machine rather than human interactions. **Customer Journey Visibility** • Harness intelligence from upstream behaviors to make more informed decisions at payment, and feedback bot behaviors from downstream interactions to enhance risk decisions upstream. **Real-time Remediation** • Take real-time action by triggering a step-up, blocking access or dynamically throttling traffic to slow down bots. • Proof of work scenarios to force bots to use up CPU time.	• Darwinium worked with a global gaming operator to uncover hard-to-detect bots that could bypass CAPTCHAs on its bonus redemption page. Behavioral biometrics were layered on top of the existing CAPTCHA solution to compare a user's current behavior to that of the wider population of users on the same page to discover anomalies indicative of fraud. • Pitney Bowes, a global shipping and mailing company, was experiencing complex bot attacks that were bypassing existing CAPTCHA-based controls, adding unnecessary friction for good users. • Darwinium sits further up the customer journey to profile traffic as it hits Pitney Bowes, detecting and providing recommendations on malicious bots, credential testing and account takeovers in real time without the need for additional step-ups. • Over 100,000 risky interactions, including a large attack, detected in one month	Abusive Accounts with righful owner in control ↓ Unauthorized Account Access ↓ Bot Detection ↓ Abuse Protection

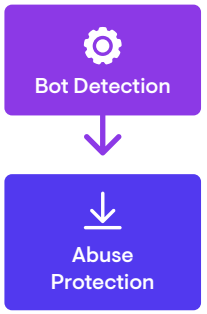
Threat	Existing Solution Shortfalls	Darwinium Capability / Benefits	Darwinium Proof Points	Use Case
Credential stuffing and PII abuse • Data breaches remain an omnipresent threat for global digital business, and almost every person who transacts online will have been exposed to some level of data theft. • Fraudsters build stolen identity data into vast lists of saleable identities on the dark web, which are used in credential stuffing attacks globally. • Social engineering is then used simultaneously to glean missing pieces of PII, or one-time passcodes (OTPs) needed to infiltrate a user account. • Fraudsters have become adept at passing KYC checks using stolen credentials, building credit histories, forging documents using generative AI, and using phishing and smishing techniques to dupe legitimate customers into divulging sensitive credentials or validating third-party checks. • Stolen credit card data can be used to register for a paid-for account (for example a streaming service) that is then sold on for a profit.	• Many fraud solutions risk-assess identity information at the point at which a new account is being created, without context of what the user has done prior to this interaction. • Static KYC checks can be easily bypassed by fraudsters, while passive digital identity checks can be fooled using stolen identity data.	**Behavioral Identification** • Incorporate behavioral analytics from journey / transaction behaviors and behavioral biometrics to better understand user identity beyond fixed identity data. **Anomaly Detection** • Uncover suspicious connections between users and accounts, such as multiple accounts attached to one email address or device • Identify high velocity / unusual login attempts indicative of bot attacks or account takeover • Seamlessly integrate third-party identity verification checks to augment behavioral identification at key points in the customer journey. • Dynamically tailor responses and remediation strategies according to risk.	• Digital signatures uncover connections between devices, locations, email addresses and online behaviors that can indicate stolen / spoofed credentials being used across new account creations and logins.	Accounts impersonating Real Entities ↓ Unauthorized Account Access ↓ Payment Fraud ↓ Abuse Protection
Man-in-the-Middle Attacks • Man-in-the-middle (MITM) attacks can take many guises, and are used to intercept communications or data between an end user and an organization for nefarious purposes. • Fraudsters will often use replica websites or email communications to gather or intercept credentials to use in attacks downstream, such as login and password data for a bank account, or OTPs to authenticate a user's identity. • These attacks are being facilitated by generative AI tools that create near-perfect replicas of images and text to increase the apparent authenticity of the dupe.	• Solutions typically focus on encouraging users to download antivirus software, use VPNs, avoid using unsecured WIFI networks and avoid reusing passwords. • The challenge with these solutions is twofold: they are based on user compliance, and they typically still rely on static data intelligence / point-in-time risk assessments based on fixed identifiers.	**Behavioral Analytics** • Analyze user behaviors from browsing and pre-authentication activities, and across user journeys, to better separate trusted and anomalous behaviors beyond simply looking at fixed identity data. **Anomaly Detection** • Uncover suspicious activity indicative of session hijack, IP spoofing, or use of stolen identity credentials. **API Abuse Detection** • Detect, monitor and protect APIs as they are added or modified across digital journeys, identifying instances of API abuse that might indicate access to backend processes or services • Referrer detection, handshake anomaly detection and sophisticated IP analytics to determine whether seemingly legitimate traffic is originating from a MITM gateway or frontend.	• A customer observed a MITM attack where a site was being proxied, but altered to collect valid user credentials and pass those onto a fraud ring. • Darwinium was able to identify anomalies in the requestor IP vs profiled IP address to identify and block the MITM attack.	Abuse Protection ↓ Scams

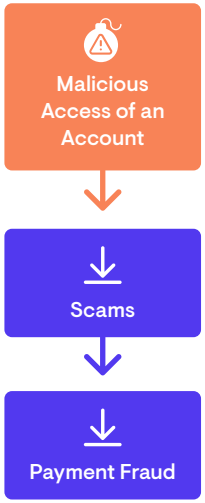
Threat	Existing Solution Shortfalls	Darwinium Capability / Benefits	Darwinium Proof Points	Use Case
Malicious Scripts / Cookie Theft • Malicious scripts are pieces of code used by fraudsters to perform harmful actions such as executing or downloading Malware, stealing personal credentials or deleting / altering files. • These attacks can often be a precursor to a future account takeover attack on an end user's account, using stolen credentials or other phished intelligence. • Cookie theft, also called session hijacking, is when an attacker steals a victim's session cookies to gain unauthorized access to their web session. • LLMs are being used to scale phishing scams to unprecedented volumes, with models trained to run conversations with unsuspecting victims and extract PII that is used for subsequent account takeovers or identity theft.	• While secure coding practices and use of HTTPS can encrypt data in transit, many malicious script attacks and cookie theft attacks use traditional malware, malicious browser extensions or .pdf documents.	**Anomaly Detection** • Identify instances of cookie theft or session replay, by detecting anomalies related to devices, locations or behaviors of a trusted user versus a potential threat. Apply this risk assessment across every step in the account security risk assessment, rather than at specific moments in time. • Identify suspicious deviations from trusted user behavior that might indicate the use of stolen credentials via malicious scripts. Compare these to normal deviations in user behavior from legitimate scenarios such as changes to locations or login behaviors, using Darwinium digital signatures. • Extend the use of digital signatures similarity matching, to uncover suspicious links between entities that could indicate the same fraudster manipulating multiple users, even when cookies are wiped, or proxies / emulators are in play.	• Darwinium worked with a Marketplace customer who leveraged long session cookies to minimize user friction when making purchases. • It was discovered that a number of user accounts were experiencing cookie replay, where a previously unseen device was using existing session cookies to bypass logins, and access other authenticated parts of the application. • Darwinium mapped journey steps on various parts of the site that included rules, to compare device attributes and behavior to those of the device that had previously logged-in successfully to the site (even if it was days or months in the past). • This provided the ability to invalidate session cookies where an anomaly had been detected. • Furthermore, our JavaScript SDK was able to enumerate installed extensions. Data lookback was also able to identify an extension that was being used to steal credentials. • The inclusion of Darwinium's Secure ID was also better able to identify cookie theft in the system without the need to implement a nonce/challenge-based cookie system in the underlying application.	

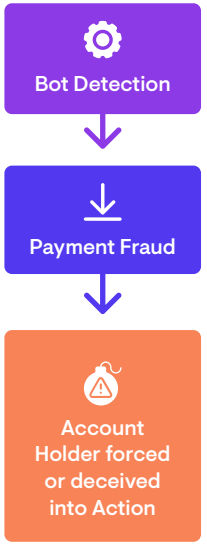
Threat	Existing Solution Shortfalls	Darwinium Capability / Benefits	Darwinium Proof Points	Use Case
Remote Access Attacks • Remote access tools are used legitimately by many end users and organizations for IT access and support. However, fraudsters also use the very same tools to gain control of customer devices to capture login credentials and take over an account. • Presence of new remote access software that has not previously been activated on an account can indicate a potential account takeover attempt. • Remote access software is often used as part of an authorized push payment (APP) fraud or scam, under the guise of supporting an end user to secure their account or prevent a fraud attack taking place.	• While some solutions can detect the presence of remote access software, they often fail to separate trusted and nefarious use. • Existing solutions also don't always combine the presence of remote access with other behavioral intelligence across the customer journey, to identify instances of scams or account takeover.	**Detection of new Remote Access Software** • Darwinium can analyze screen refresh rates, and other attributes, to passively detect whether remote access is present on a user session. • Darwinium also has an API integration with AnyDesk, which can be called as part of a potential scaam journey, to understand whether there is a live AnyDesk session active. **Layered Behavioral Analytics to Identify Scam-like Behaviors** • Identification of remote access software can be layered with behavioral analytics to detect anomalies that might indicate a scam payment journey, such as unusual pauses or hesitations, new beneficiary creation, indicators that the user is being guided or coerced through a payment, or unusual payment transaction anomalies around velocities and amounts.	• Darwinium's device profiling was able to identify a series of users on a fintech website where there had been an abrupt change in the users' screen refresh rate and mouse movement biometrics. • This suggested the use of a remote access tool. A list of compromised users was then labelled and contacted by the vendor where their credentials were updated.	

Threat	Existing Solution Shortfalls	Darwinium Capability / Benefits	Darwinium Proof Points	Use Case
Content Spoofing / Content Fraud • Fraudulent content - fake listings of dream holidays or sought after products, scam reviews on marketplaces, or fake emails / SMS messages, can severely damage brand reputation and customer trust, as well as support account takeover attempts via phishing and smishing or sensitive customer credentials. • Fake or duplicate content can be particularly hard to detect in the age of AI, as tools such as ChatGPT and Midjourney can create perfect replicas of trusted brand content, or alter reviews or listings en masse to create limitless fraudulent listings.	• Content fraud is notoriously hard to uncover, and often relies on manual reviews and feedback from customers to remove harmful content after it has appeared on a website. • Automated generative AI tooling can typically recreate and execute fraudulent content faster than it can be reviewed and removed. • While many solutions can detect unusual listings from the same devices or email addresses, few combine this with behavioral or similarity matching of text and images to detect complex, automated attacks.	**Detect Image and Text Anomalies** • Darwinium Digital Signatures for text and image similarity matching can be compared in real time to previous signatures. These can identify unusual consistencies in text and images across multiple listings / accounts, even if a fraudster has attempted to make them look significantly different.	• A digital signature changes with changes to a base image. This algorithm can be applied across text similarity to uncover reviews or listings that are too similar to be legitimate, but are not picked up as an exact duplicate.	Abuse Protection ↓ Scams
Social Engineering / Phishing / Smishing • Social engineering tactics are being combined with more traditional brute force account takeover techniques to bypass additional authentication checks put in place to protect user accounts. • Fraudsters are socially engineering users to divulge either login credentials, or one-time passcode (OTPs) used to check the risk of a new device logging in to an account. • Social engineering is also being used at scale in scams and authorized push payment (APP) fraud, to convince users to make payments for goods or services that don't exist. Given the trusted user is making the payment, businesses can't simply rely on device or location anomalies to detect a traditional account takeover attempt.	• Existing fraud detection solutions focus on anomalies in device and location behavior that indicate potential account takeover or payment fraud scenarios. • There are very few solutions on the market that can successfully detect social engineering behaviors because they don't consider intent data, and behavioral analysis. • Those that do incorporate behavioral analytics tend to do so at specific points in the customer journey, rather than holistically across every touchpoint. • Social engineering and scam journeys tend to be better identified by looking at behaviors and customer intent signals across every interaction, rather than at moments in time.	**Behavioral Analytics Across the Customer Journey** • Darwinium can piece together intent and behavioral data to understand deviations from normal user behavior that may indicate coercion or social engineering. This might include delays or hesitations, live call detection, payment volume or velocity anomalies or login frequencies. **Dynamic Tailored Messaging** • Darwinium can alert the customer to potential risk earlier in the social engineering cycle with tailored messages according to customer needs. This can help to disrupt warning fatigue and alert blindness while introducing appropriate friction for high-risk payments.	• Darwinium's device profiling was able to identify a series of users on a fintech website where there had been an abrupt change in the users' screen refresh rate and mouse movement biometrics. • This suggested the use of a remote access tool. A list of compromised users was then labelled and contacted by the vendor where their credentials were updated.	Unauthorized Account Access ↓ Authorized Account Access ↓ Scams ↓ Payment Fraud

Threat	Existing Solution Shortfalls	Darwinium Capability / Benefits	Darwinium Proof Points	Use Case
Deepfakes • The speed at which deepfake technology is advancing to create near perfect replicas of human images, voices and videos has accelerated the risk they pose to digital businesses. • Fraudsters are able to create pictures, skeleton fingerprints, voice recordings and liveness checks to bypass the most sophisticated biometric-based identity verification and authentication checks. • Deepfakes are also being successfully used by fraudsters in scams to convince both employees and loved ones to transfer money under the guise of legitimacy.	• Many identity verification solutions rely on elements of biometrics to link a person's static identity data with their physical identity as they apply for a new account, product or service. • The challenge that deepfake technology poses, is that it makes this layered approach redundant – static identity data can be stolen or spoofed, and physical identity checks can be deepfaked. • An additional challenge that many digital businesses face is that at a new account creation event, there is often little digital intelligence available to ascertain the trust or risk of a new user. • During login or payment events, biometric authentication can be bypassed with deepfake images, fingerprints or voice commands.	**Risk Context from Browsing and Pre-Authentication** • Darwinium gathers intelligence across the complete customer journey, from the moment a user lands on your site. This means businesses can gather additional rich behavioral intelligence about a user before they apply for a new account or log in. • Darwinium can layer behavioral and device techniques with traditional KYC integrations, for a more accurate risk decision. • Trusted users typically behave differently from fraudsters, browsing and interacting with a website in a different way. **Behavioral Identification** • Rather than relying on static pieces of identity data, biometrics checks or isolated pieces of digital identity intelligence, Darwinium uses the full context of user behavior across every interaction point to separate trusted user behavior from a potential deepfake.	• Darwinium's behavioral identifiers were used to identify a ring of click farm users who had been signing up for multiple accounts. • This identification resulted in manual review for subsequent accounts, and the ability to blocklist further attacks. • Further, the use of in-built image hashing was leveraged to further protect calls to the KYC verification solution, preventing unnecessary calls where a repeated image / credentials had been used.	

Threat	Existing Solution Shortfalls	Darwinium Capability / Benefits	Darwinium Proof Points	Use Case
Bonus Abuse • Fraudsters continually look for opportunities to exploit promotional offers, bonuses or incentives provided by, online gaming operations, eCommerce merchants and banks / credit card providers. • These can include sign-up or referral bonuses, credit card rewards, free trials or matched rewards. • Fraudsters uses automated bots and scripts to exploit bonuses at scale, as well as using proxies, emulators, and CAPTCHA solvers to bypass detection.	• Existing bonus abuse solutions focus on detecting automated attacks, but can't always detect the more sophisticated bots that are tuned to bypass rate control measures, or solve CAPTCHA-based puzzles designed to deter automated traffic. • In addition, once one vulnerability is plugged, fraudsters typically pivot their attack profile to target a new vulnerability such as an exposed backend API or a new bonus offer. Businesses are then tied to code-changes to cover new touchpoints or pages on their website, which can take weeks or months.	**Bot Detection** • Detect sophisticated low-and-slow bots and scripts that are being used to abuse bonuses intended for trusted customers. • Identify multiple accounts coming from the same device or location, even if they are wiping cookies or using proxies / emulators to evade detection. • Remove the requirement to use expensive CAPTCHA-based solutions on every interaction, reserving step-ups for genuinely high-risk interactions. **Time Confidence Features** • Use advanced features to determine usage and frequency throughout a given time window, and determine variances or anomalies in behavior in comparison to the full cohort of users. Use this to determine potential bots or click farm users. **Digital Signatures** • Detect previously unseen connections between users that might indicate collusive behavior or an organized fraud ring. **Real-time Customer Journey Protection** • Protect new touchpoints in the customer journey by defining journey and data mapping behaviors from within the Darwinium portal. Remove reliance on engineering resource to make code changes. Protect new vulnerabilities instantly.	• The scenario below shows a bonus abuse attack that Darwinium detected for a global gaming company, that links multiple apparently unconnected smaller attacks to the same fraudster, exposing the scale of the attack. • Darwinium helps to expose this behavior by matching device, location identity and behavioral intelligence by similarity rather than an exact match, uncovering the use of proxies, emulators and cookie wiping that fraudsters typically use to avoid detection.	

Threat	Existing Solution Shortfalls	Darwinium Capability / Benefits	Darwinium Proof Points	Use Case
Loyalty / Rewards Fraud • Fraudsters are increasingly seeing loyalty-based accounts as a lucrative opportunity to make money. Loyalty and rewards points can often be converting into products, flights or hotel bookings that can be monetized via sale, refunds or transfers. • Loyalty fraud can take a variety of forms, but will typically involve either a fraudulent new account creation or a takeover of an existing loyalty-based account. • eCommerce merchants and online travel agencies (OTA) are seeing a growth in account takeovers and loyalty fraud. Many organizations have focused on solutions to prevent payment fraud, which has pushed fraudsters to exploit other vulnerabilities in the customer journey.	• New account creation for the purposes of exploiting loyalty or rewards bonuses can be particularly hard to detect, given there is often very little information available when a new user registered for an account. Existing solutions tend to focus on static identity verification checks that can be easily bypassed by fraudsters in possession of stolen credentials. Many solutions fail to analyze behaviors prior to a new account creation that might indicate nefarious intent. • Fraudsters are adept at combining brute force account takeover attempts with social engineering to bypass existing solutions that are in place to detect unauthorized account access. • Most account takeover solutions focus on identifying a new or high-risk user accessing a trusted account, but they can be fooled by stolen or spoofed credentials, private browsing, cookie wiping, proxies and emulators.	**Risk Context from Browsing and Pre-Authentication** • Darwinium can gather additional behavioral intelligence about a user, or fraudster, before they apply for a new account, identifying high-risk scenarios such as unusual navigation or timing behaviors that deviate from typical user behavior. **Continuous Monitoring and Real-time Decisioning** • Continuous risk-based authentication across the entire user journey, incorporating network, device, location, identity and behavioral biometrics intelligence. • Introduce additional authentication checks for high-risk interactions, block risky logins in real time, reduce friction for trusted returning users. • Identify unusual changes in customer details, or new redemption behaviors that might indicate an account takeover scenario, such as transfer of rewards to a new user. Compare to previous redemption behaviors. **Digital Signatures** • Improve returning user recognition rates based on the context of an interaction. • Optimize challenge rates with customer experience, while reducing false positives. Condense granular data relating to devices and behaviors into signatures that can be compared for similarity to previous and known bad interactions. **Geo-location Intelligence** • Understand network changes relating to IP address, internet provider, connection type and proxies which might be indicative of an account takeover scenario. • Detect logins from new or unusual locations: detailed context on the location of devices, addresses, proxied and true IP addresses, as well as suspicious account changes e.g. unusual new shipping addresses.	Darwinium accurately detected a series of account takeover attempts at an eCommerce site, by layering information related to devices, locations and behavioral biometrics. • A series of risky logins were identified that resolved back to the same individual attempting to bypass device recognition. Despite registering “new” device information across multiple logins, the digital signature of the user was consistent. (See screenshot below). • This was supported by the fact that the behavioral biometrics data indicated that it was the same fraudster attempting to access multiple accounts across several account takeover attempts. • Darwinium location intelligence also identified a mismatch between the user’s stated location - that was attempting to mimic the account owner’s behavior - and the actual login location.	

Threat	Existing Solution Shortfalls	Darwinium Capability / Benefits	Darwinium Proof Points	Use Case
Card-not-present Fraud • Protection of online payments has advanced significantly, particularly with the explosion of payments made via digital wallets and apps on mobile devices that are protected by the on-device biometrics authentication protocols. However, this evolution has simply prompted more complex attacks. • Fraudsters leverage stolen card data to make fraudulent card-not-present payments, combining card testing with social engineering to convince customers to divulge OTPs mandated by strong customer authentication (SCA) protocols such as PSD2. • Authorized push payment (APP) fraud, also known as scams, has become pervasive, with fraudsters persuading customers to make a payment for a phony purchase, investment or service, thereby bypassing traditional anomaly detection rules, such as changes to devices or locations.	• While many payments fraud solutions work excellently to detect typical payment fraud scenarios such as the use of a stolen credit card, fraudsters are adept at pivoting their attacks to avoid detection. • Social engineering attacks are being used to move customers off a trusted platform to make a payment, convince them to make an authorized payment to a fraudster, or to divulge login credentials or OTPs to allow the fraudsters to make an authenticated payment on their behalf. • It is these types of behaviors that are particularly hard to detect, because they are bypassing all known payment authentication protocols that are designed to detect unauthorized behavior.	**Behavioral Intelligence Across the Complete Customer Journey** • Darwinium provides eCommerce merchants with intelligence and context from upstream interactions to better inform risk assessments at payment, including behavioral intelligence that might indicate unauthorized access or a social engineering attempt. Intelligence related to typical payment patterns and velocities, journey times, and behavioral biometrics data can add additional context to checkout and payment events. **Dynamic Remediation** • Integrate additional third-party payment authentication services in real time via the Darwinium Marketplace. • Alert customers to potential risk earlier in the social engineering cycle with tailored messages that relate to the payment they are trying to make.	• Darwinium's journey insights were able to protect against bot abuse, targeting a credit card pre-authorization end point for card testing on a merchant's payment workflow. • This was done by identifying journeys where the API endpoint was being hit without corresponding upstream site activity / no prior steps in the customer journey. • While simple in this instance – this contextual knowledge was highly effective in blocking direct endpoint abuse in ways conventional cyber solutions (lacking context beyond the API call itself). could not.	

Threat	Existing Solution Shortfalls	Darwinium Capability / Benefits	Darwinium Proof Points	Use Case
Business Logic Abuse • Business logic abuse exploits flaws or loopholes in the intended workflow, processes, or rules of a system for financial gain or to steal sensitive customer data. • Examples include account sharing, returns fraud, bonus abuse, free trial exploitation and coupon stacking.	• Many examples of business logic abuse are not fraudulent per se, but can damage brand reputation, customer trust and a business's bottom line. • Businesses need a highly flexible and configurable solution that can be tuned to detect abuse scenarios specific to each business.	**Bot Detection** • Detect sophisticated low-and-slow bots and scripts that are being used to exploit rewards, incentives or bonuses intended for trusted customers. • Identify multiple accounts coming from the same device or location, even if they are wiping cookies or using proxies / emulators to evade detection. **Digital Signatures** • Detect previously unseen connections between transactions or users that might indicate exploitation of business processes, such as multiple returns from the same shipping address, or multiple shipping addresses attached to one user trying to obfuscate their identity. **Flexible, Configurable Decision Engine** • Darwinium's highly configurable decision engine allows businesses to tailor decisions and actions based on their individual use case and business need. Journeys, features, rulesets and models are configurable by no-code GUIs, low-code or full code options to suit all user groups. Use either a drag and drop interface, or a developer-friendly VSCode-based integrated development environment (IDE).	• Darwinium's journey-wide visibility enables policy authors to leverage context in each interaction (including page loads and API requests). • Using the combination of features that trigger when a given identifier re-uses an API, and the ability to determine whether a previously executed step (a page load) had been performed, Darwinium can identify instances where end-users have been reverse-engineering the API (presumably to get it to leak information over many interactions) and block subsequent traffic requests.	Abuse Protection

Threat	Existing Solution Shortfalls	Darwinium Capability / Benefits	Darwinium Proof Points	Use Case
API Abuse • New APIs and microservices are being added to websites regularly. As a result API traffic is growing significantly faster than web traffic, making it harder to catalogue, track and maintain. • APIs significantly increase the potential attack surface of an organization. Yet without clear visibility of all API traffic, it becomes harder to detect attacks, exploitation, or abuse of business logic. • Adversaries, whether insider threats or fraudsters, see the opportunity that this environment creates. API vulnerabilities potentially allow them to bypass authentication, steal sensitive data, and abuse incorrect or misconfigured business logic.	• The speed with which digital businesses are adapting services and processes has exposed many backend APIs to risk. Many remain exposed simply because they haven't been mapped or documented, leaving them unprotected by existing solutions. • Many API security solutions focus on binary controls such as rate limiting measures, IP or network-based traffic analysis, or authentication protocols at specific moments in time. • However, fraudsters have become adept at bypassing many of these controls, simply scanning for new vulnerabilities in the customer journey downstream.	**Bring Downstream Context to the Perimeter Edge** • Darwinium can be integrated with API gateways or edge networks for complete visibility of traffic going to and from an endpoint. • Bring the context of downstream events to the security perimeter, to better discover, monitor and maintain new and existing API connections. **Behavioral Profiling of APIs Across Digital Journeys** • Detect anomalies in new and existing API behavior against a broader business context, separating intended operations from nefarious intent. • Harness a fuzzy API user signature that is independent of the host, leveraging features such as: • Content ordering • White space • Optional parameter presence • Other formatting • Header information • Leverage full behavioral profiling on every API request to generate features and signals which detect normal and anomalous API behavior at each step of a digital journey. • Detect scenarios where an API is being called correctly and in the correct sequence but shows anomalies between the entities and relationships being used in the API sequence, for example between the location of a card issuing bank and the purchase.	• Darwinium's journey insights were able to protect against bot abuse, targeting a credit card pre-authorization end point for card testing on a merchant's payment workflow. • This was done by identifying journeys where the API endpoint was being hit without corresponding upstream site activity / no prior steps in the customer journey. • While simple in this instance – this contextual knowledge was highly effective in blocking direct endpoint abuse in ways conventional cyber solutions (lacking context beyond the API call itself). could not.	Abuse Protection

The Darwinium Difference:

Protect the Entire Customer Journey:

Darwinium provides complete visibility of user behavior across the entire customer journey, from pre-authentication and browsing behaviors, through every digital interaction a user makes on a website. Simple deployment options cover your content delivery network (CDN), web, mobile apps and APIs, removing pressure on IT resource and decoupling remediation from release cycles.

Remove Data Siloes:

Consolidate multiple data siloes into a single source of truth across the customer journey. Add network, device, behavior and endpoint context to security tools, and complete journey-level visibility and context to fraud teams for a complete cyberfraud prevention solution.

A New Approach to User Recognition:

Use Darwinium digital signatures to identify more users without adding unnecessary friction. Tune recognition rates based on context, from faint suspicion to absolute certainty. Sets of granular forensic data, like device, swipe and keyboard interactions are condensed into a corresponding signature for easy similarity comparison. Built on a continuous scale of similarity from zero to one, rather than on a fixed identifier, digital signatures optimize challenge rates with customer experience while reducing false positives.

See Beyond Identity to Understand Intent:

Use Darwinium's behavioral identification to incorporate behavioral analytics and behavioral biometrics data to better understand unusual or anomalous behaviors. Identify hard-to-detect fraud such as social engineering and scam behaviors by comparing current behaviors to previous behaviors and known bad interactions.

Make Agile Risk Decisions:

Move seamlessly from analytics to action, with real-time customer journey orchestration - featuring an integrated decision platform, plug and play third-party integrations and dynamic, tailored remediation.

Reduce Deployment Effort:

Integrate at the perimeter edge, via CDN infrastructure, to protect the complete customer journey. Darwinium only needs to be deployed once. Business users can then tailor and adapt new journeys and configurations directly within the product thereafter.

Privacy-by-Design:

Darwinium gives businesses the option to move data classification, encryption and anonymization to the perimeter edge. Retain full control of sensitive data, with less exposure to risk. Darwinium uses a fully anonymized version of this data that can be processed globally for security and fraud prevention purposes. The original data is not recoverable.

Glossary

Darwinium Capability / Benefits			
Account Security Abuse Types	**Account Security Abuse Sub-Types**	**Methods to achieve Account Security Sub-type**	**Example Downstream Harms**
Abusive Accounts with rightful owner in control (i.e., Accounts on a platform, website, or service with malicious intent or in violation of the platform's terms and conditions)	**Accounts using Fake Information** (i.e. Accounts using information (e.g., name, tax identification number etc) that is not real)	**Bots:** Bots can be utilised at automate the creation and control of Fake Accounts **Humans:** Humans working individually or in a group (e.g., click farm) can create and control fake accounts	**Fake accounts can be utilized in a variety of downstream abuse types, such as:** • Payment Fraud: Used in a variety of payment fraud abuse vectors such as testing stolen credit card details for validity by making small transactions, or to execute chargeback schemes, where fraudulent purchases are made and later disputed to recover funds. • Phishing Schemes: Tricking users into providing sensitive information like passwords and credit card details by impersonating trustworthy entities (e.g., businesses or individuals) • Spreading Disinformation: Distributing false news and propaganda to influence public opinion, sow discord, or manipulate perceptions on social, political, or economic issues. • Cyberbullying and Harassment: Anonymously targeting individuals for bullying, harassment, or intimidation. • Boosting Fake Engagement: Creating artificial popularity by inflating likes, shares, and followers on social media.
	Accounts using Fake Information (i.e. Accounts using information (e.g., name, tax identification number etc) that is not real)	**Bots:** Bots can be utilised at automate the creation and control of accounts impersonating real entities **Humans:** Humans working individually or in a group (e.g., click farm) can create and control accounts impersonating real entities	**Accounts impersonating real entities can be utilized in a variety of downstream abuse types, such as:** • Phishing Attacks: Tricking individuals into revealing sensitive information like login credentials, financial data, or personal identification by pretending to be a trusted organization. • Spreading Misinformation: Disseminating false or misleading information under the guise of a credible source to manipulate public opinion or cause panic. • Financial Fraud: Registering for financial schemes using another entity's tax information, causing that entity (e.g., a business) to receive tax forms for income they never generated. • Social Engineering: Gaining trust and manipulating victims into taking actions they wouldn't normally take, such as transferring money or sharing confidential information. • Reputation Damage: Damaging the reputation of a person, business, or organization by spreading false statements or engaging in unethical behavior while impersonating them.
	Accounts controlled by bad actors but using legitimate details (i.e., The account was registered by an entity using real information that they have a legitimate right to be using but the intention of the actor/s in control of the account is malicious)	**Bots:** Bots can be utilised at automate the creation and control of accounts impersonating real entities **Humans:** Humans workingw individually or in a group (e.g., click farm) can create and control accounts impersonating real entities	**Accounts controlled by bad actors but using legitimate details can be utilized in a variety of downstream abuse types, such as:** • Distributing false news and propaganda to influence public opinion, sow discord, or manipulate perceptions on social, political, or economic issues. • Payment Fraud: Used in a variety of payment fraud abuse vectors such as testing stolen credit card details for validity by making small transactions, or to execute chargeback schemes, where fraudulent purchases are made and later disputed to recover funds. • Phishing Attacks: Tricking individuals into revealing sensitive information like login credentials, financial data, or personal identification by pretending to be a trusted organization even if its a entity that the bad actor has a legitmate right to be using (e.g., a business that have registered)

Darwinium Capability / Benefits			
Account Security Abuse Types	**Account Security Abuse Sub-Types**	**Methods to achieve Account Security Sub-type**	**Example Downstream Harms**
Malicious Access of an Account (i.e., people or systems gain access to an account they have no legitimate right to be accessing)	**Authorised Account Access** (i.e., The legitimate owner of the account knowingly gives access to their account to another person with malicious intent)	**Social Engineering:** By exploiting trust, authority, urgency, or curiosity, social engineers manipulate individuals into willingly providing their credentials, often without realizing they are being deceived. This can be executed through humans, bots, or a combination of both.	**Accounts where the legitimate owner of the account knowingly gives access to their account to another person with malicious intent can be utilized in a variety of downstream abuse types, such as:** • Data Breach: Sensitive personal or financial data stored within the account may be exposed to unauthorized parties or leaked. • Fraudulent Transactions: The malicious actor could make unauthorized purchases, transfers, or other financial transactions, leading to financial losses. • Escalated Security Risks: The malicious actor may use the access to compromise other related accounts (e.g., by resetting passwords, accessing linked services). • Loss of Access: Attackers may change passwords or security settings, locking the rightful owner out of their own accounts. • Spam: The malicious actor can use the account to send unsolicited bulk messages, promoting scams, phishing links, or malicious content to the account holder's contacts or wider audience. • Scam: The attacker can leverage the account to impersonate the owner and deceive others into providing money, personal information, or other sensitive data through fraudulent schemes, such as fake investment opportunities or emergency requests. • Misinformation: The malicious actor can use the account to spread false or misleading information, which can harm the credibility of the account owner and contribute to the spread of inaccurate narratives, potentially causing confusion or harm to others.
		Incentives: The legitimate owner may be offered money or rewards to provide access to their account. For example an employee working for a business might sell access to the company's social media account in exchange for a financial reward.	
	Un-authorised Account Access (i.e., The account is accessed without the rightful owner's knowledge)	**Phishing:** Using fraudulent emails, SMS (smishing), or calls (vishing) to trick users into providing login credentials through fake websites or malicious links.	
		Credential Stuffing: Using stolen usernames and passwords from previous data breaches to attempt logins on multiple platforms, relying on password reuse.	
		Brute Force Attack: Automated tools systematically try all possible password combinations until the correct one is found, typically targeting weak or simple passwords.	
		Keyloggers: Malware that records keystrokes, capturing login credentials as they are typed and sending them to the attacker	
		Session Hijacking: Stealing session cookies to take over an active session without needing the victim's login credentials, allowing unauthorized access.	
		SIM Swapping: Convincing a mobile provider to transfer the victim's phone number to a new SIM card under the attacker's control, allowing interception of SMS-based Two-Factor Authentication (2FA) codes, which can lead to unauthorized access of accounts.	
		Recycled Email Account Takeover: Exploiting old or inactive email accounts that have been reassigned or recycled, allowing attackers to reset passwords on linked accounts (e.g., social media, banking) by receiving password reset emails, thus gaining unauthorized access to the victim's accounts.	
		SQL Injection: Exploiting vulnerabilities in a website's authentication system by injecting malicious SQL queries into login fields, allowing attackers to bypass login authentication, retrieve or modify account credentials, elevate privileges, and gain unauthorized access to user or administrative accounts.	

Darwinium Capability / Benefits		
Account Security Abuse Types	**Methods to achieve Account Security Sub-type**	**Example Downstream Harms**
Malicious Access of an Account (i.e., people or systems gain access to an account they have no legitimate right to be accessing)	**Social Engineering:** Attackers manipulate or deceive the account holder using tactics like phishing, impersonation, or psychological manipulation to gain access or trick them into taking harmful actions. **Forced Coercion:** Attackers use threats, blackmail, or financial pressure to force the account holder into performing specific actions, such as granting access or transferring money, against their will.	**Accounts where the owner is forced or deceived into Action can be utilized in a variety of downstream abuse types, such as:** • Payment Fraud: Attackers may pressure or manipulate the account holder into transferring funds or making purchases on their behalf, resulting in financial harm. • Data Theft: The account holder may be deceived or coerced into handing over sensitive personal or organizational data, which can then be exploited or sold. • Spreading Malware: The account holder could be duped or compelled into sharing malicious software through their account, spreading security risks to contacts and networks. • Phishing and Scams: Attackers can mislead or coerce the account holder into sending phishing emails or scam messages to their contacts, leveraging the trust linked to their legitimate account. • Compromising Linked Accounts: The account holder may be tricked or pressured into granting access, allowing attackers to infiltrate other linked accounts or platforms, such as social media or financial services. • Facilitating Money Laundering: Attackers may deceive or compel the account holder into unknowingly conducting illegal financial activities, such as laundering money. • Reputation Damage: The account holder could be manipulated or pressured into actions that tarnish their reputation, such as posting offensive content or sending harmful messages.