A CISO's Guide to Cyberfraud Protection

How C-level leaders can unify cybersecurity & fraud teams to outpace AI-powered attacks

DataDome

Table of contents

Fraud has changed: Faster, smarter, harder to detect 3

What is cyberfraud protection? 5

A new defensive posture 10

Viewing the world through the eyes of the attacker 10

The types of cyberfraud 11

Cyberfraud attacker framework: How cybercriminals operate 14

A new approach to defense: Cyberfraud fusion 19

The need for intent-based detection in the AI era 19

Organizational structure: Aligning to the attacker's framework 20

Why legacy fraud tools can't keep up 23

Cyberfraud protection: Core solutions, capabilities, & platform selection 24

The solutions that make up cyberfraud protection 24

The cyberfraud protection maturity model 25

The future of cyberfraud protection: AI-driven, real-time, & built to adapt 29

Why DataDome is leading the future of cyberfraud protection 31

Stopping cyberfraud before it happens 33

Fraud has changed: Faster, smarter, harder to detect

There was a time when fraud and cybersecurity could be handled separately.

Fraud teams focused on manual transaction reviews and chargebacks. Security teams protected the infrastructure and stopped attacks. The scale was smaller. The attacks were simpler. And the tools, predominantly siloed, static, and rule-based, were often enough.

That time is over.

Fraud has become inseparable from cybersecurity, and effective fraud mitigation now depends on security controls that can detect and stop fraudsters upstream in real time, before they're able to cause downstream problems.

Modern fraud campaigns have moved beyond stealing credit cards or abusing return policies. They now operate at a greater scale and speed, working across the full user journey, from sign-up to login to checkout. They leverage bots, automation, and now AI, including agentic AI, to mimic real users, adapt their attack tactics in real time, and evade detection. Increasingly, they target business logic in sites, apps, and APIs, exploiting the very workflows, promotions, and features that companies build to drive growth.

While attackers execute seamless, multi-stage, multi-tool operations, defenses remain fragmented. Siloed teams and disconnected tools leave critical intelligence and protection gaps. According to Gartner®[1], "complexity is the enemy of security; yet the average organization works with 10 to 15 security vendors and 60 to 70 security tools. And many of these products have similar capabilities, making it easy for misconfigurations to occur and difficult to uncover security gaps and integrate the products." These include tools for cybersecurity, fraud, identity, bot mitigation, payment fraud, case management, and customer service.

Gartner® Disclaimer

[1]Gartner, Simplify Cybersecurity With a Platform Consolidation Framework, Dionisio Zumerle, John Watts, 26 March 2024. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved

This operational complexity and tools fragmentation benefits attackers, who act without regard for team boundaries.

Today's fraudsters target entire technology stacks, not just isolated components, so fraud and security teams must take a holistic approach to defense. That means breaking down the walls between cybersecurity and fraud teams, and aligning strategy, tools, and data.

Enter cyberfraud protection—a new category purpose-built for the AI era. It unifies fraud and security teams under a single framework, designed to detect intent and block threats across the entire customer journey, in real time.

How to use this guide

This guide is for enterprise leaders who recognize the stakes and know that defenses must evolve.

Whether you're a CISO confronting automation at scale or a fraud leader pushing for platform consolidation, this is your playbook for adopting and implementing cyberfraud protection.

Inside, we'll break down:

- **Why the line between fraud and cybersecurity teams has permanently blurred, and why existing organizational silos are now liabilities.**
- **How legacy defenses like rulesets, static identity checks, and manual reviews are being replaced by real-time, intent-based detection.**
- **What cyberfraud fusion looks like in practice, including how teams are unifying signals and sharing systems.**
- **A maturity model to help benchmark your current posture and evolve toward integrated, AI-driven protection.**

With insights from threat research, industry benchmarks, and real-world use cases, this guide is both a roadmap and framework. It's how you operationalize cyberfraud protection across people, processes, and platforms to align fraud and security teams, cut through point-solution noise, and stay ahead in the era of AI-powered fraud and abuse.

Cyberfraud is no longer a niche concern. It's a board-level risk. And cyberfraud protection is how you meet it head-on.

What is cyberfraud protection?

Cyberfraud protection is a unified, AI-powered framework that brings security and fraud teams together through shared tools and data. It analyzes the intent behind every interaction to detect and block malicious behavior in real time, stopping threats across the entire digital user journey.

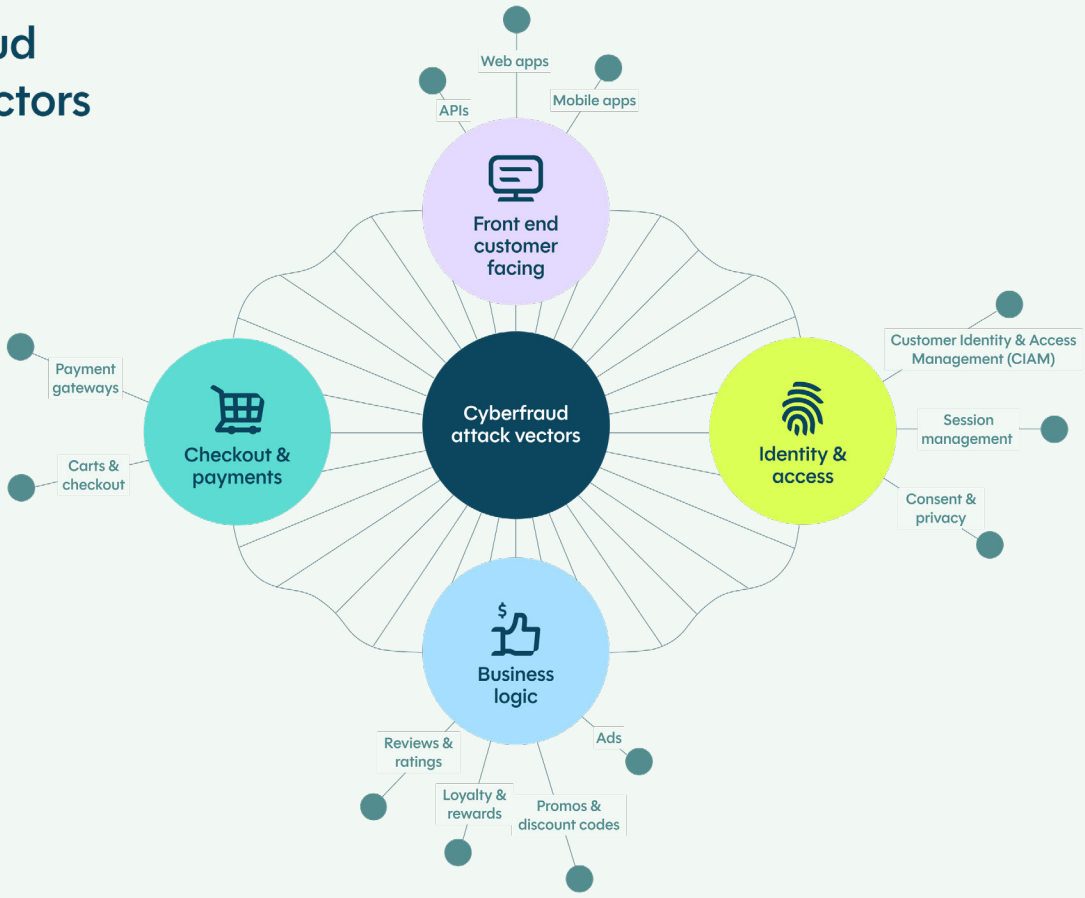
Defense must begin at the first malicious action, whether it's reconnaissance, scraping, fake account creation, or credential stuffing, and continue throughout the account lifecycle to prevent account takeover (ATO), payment fraud, and more. True protection must span all touchpoints: signup, login, checkout, mobile apps, and APIs.

The term "cyberfraud" itself emerged from a simple realization: fraud has become a cybersecurity problem.

It typically involves the use of digital technologies, particularly automated and open-source tools, to carry out deceptive or unauthorized activities for financial gain or data theft. In simpler terms, it's fraud that happens online and often involves bots, stolen credentials, social engineering, or fake identities to exploit systems, users, or businesses.

It encompasses a wide range of attack vectors that exploit vulnerabilities across the entire digital customer journey, from the front end to the backend business logic.

Cyberfraud attack vectors



As shown in the graphic, cyberfraud can target **four major layers:**

- **Front end (customer-facing):** Attackers hit mobile apps, web apps, and APIs to scrape data, probe for vulnerabilities, or simulate legitimate traffic using bots or AI agents.
- **Identity & access:** Credential stuffing, session hijacking, and abuse of Customer Identity and Authorization Management (CIAM) systems enable fraudsters to impersonate users or bypass authentication.
- **Checkout & payments:** Exploitation of technology systems, such as shopping carts and payment gateways, to commit fraudulent activities and transactions.
- **Business logic:** Exploitation of functional flaws to exploit promo codes, discounts, and customer rewards or loyalty programs.

With AI-powered tools and inexpensive "Bot-as-a-Service" platforms more accessible than ever, a single fraud operation can launch over 4 million credential-stuffing attempts in just one hour: rotating IPs, mimicking human behavior, and adapting dynamically to bypass defenses.

Cyberfraud thrives on fragmented defenses. These attacks may look different at each layer, but they're part of the same end-to-end strategy to monetize your vulnerabilities.

These attacks are no longer manual or isolated. They are automated, continuous, and global in scale, blending bots, stolen credentials, fake accounts, and abuse of business logic into one integrated playbook.

Convergence in action: Evidence for cyberfraud fusion

We're not the only ones seeing the shift.

In a recent report, Gartner characterizes the cyberfraud fusion trend (and drivers) clearly:

"Cyberfraud fusion is an emerging trend that reframes online fraud events as security incidents from which prevention frameworks can be established. Individual scams and fraudulent events are first broken down into relevant tactics, tools and procedures... The other significant portion of this trend relates to the breaking down of organizational silos between identity, security and fraud teams.

In many organizations today, these teams all rely on different data, tools, processes and people, often working in isolation on symptoms of the same problem. Adversaries exploit these gaps and cracks, causing organizations to reactively scramble to address their vulnerabilities. The approach represents a significant shift toward proactive defense and mitigation rather than the detect and respond techniques used to combat fraud online today."[2]

In fact, Gartner says that "by 2031, at least 50% of large financial institutions and online retailers will consolidate online fraud prevention personnel, duties, and responsibilities into cybersecurity teams reporting to the CISO."[3]

What changed (and why teams must adapt)

What used to look like opportunistic abuse now operates like a vast criminal SaaS enterprise: scalable, persistent, organized, and optimized by AI. AI doesn't just make fraud faster, it makes it smarter over time.

To exploit business logic and commit fraud at scale, attackers first need access, either by hijacking existing customer accounts or creating fake ones. Synthetic identities pass verification. Sophisticated bots, now enhanced by AI, navigate full user journeys undetected. Coordinated campaigns—sometimes leveraging agentic AI—chain together reconnaissance, scraping, fake account creation, and payment fraud into a single automated operation, executed seamlessly and often without triggering additional alarms.

If past threats were like digital pickpocketing, today's attacks resemble flash mob shoplifting: organized, fast-moving, and built to overwhelm. Just as brick-and-mortar retailers are rethinking storefront security, digital businesses must re-architect how they detect, block, and respond to fraud.

Target is a great example of this response. As a leading U.S. retailer with nearly 2,000 stores and over $100 billion in annual sales, they face a high level of security and fraud risks. They have publicly discussed the benefits of converging cybersecurity, risk management, and fraud prevention under unified leadership. This model, designed to accelerate threat detection and response, underscores the urgency and global relevance of aligning these functions. With shared leadership, these teams can work in a coordinated effort to stop equally coordinated attacks.

Gartner® Disclaimer

[3]Gartner, Emerging Tech: The Future of Online Fraud Prevention, Dan Ayoub, Pete Redshaw, Sean ONeill, Vatsal Sharma, 30 January 2025. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved

Real-world cyberfraud case study

Vinted, a leading peer-to-peer marketplace with over 100 million users, became the target of a sophisticated, multi-pronged fraud operation. Attackers used automated bots to launch credential stuffing campaigns and create thousands of fake accounts per week, flooding the platform with counterfeit and illicit listings. Each fake account generated thousands of fraudulent items, overwhelming moderation workflows, and damaging user trust.

What made this operation especially dangerous was its use of advanced evasion techniques. Bots rotated IPs, mimicked legitimate user behavior, and spoofed device fingerprints, particularly on mobile devices, to bypass detection. Attackers even employed paid proxy networks, emulated real Apple iPhone devices, and created sleeper accounts (registered in advance and activated weeks or months later) to increase success rates and evade traditional detection methods.

The result?

Millions in potential financial losses, increased chargebacks, a flood of moderation overhead, and potential reputational damage. To make matters worse, the attackers evolved rapidly, pivoting tactics within hours of being blocked.

This example shows how today's fraud operations aren't one-off attempts. They're structured, persistent, and AI-augmented in ways that make legacy defenses obsolete. Combating threats like this requires real-time, AI-powered cyberfraud protection that can assess intent, not just identity, and respond at the speed of the attack.

Check out 100+ other cyberfraud case studies here.

A new defensive posture

Modern cyberfraud operations blend tactics by leveraging bots, synthetic identities, and business logic abuse into a single, seamless threat chain. Defending against modern cyberfraud demands a new posture—one built on real-time AI, shared intelligence, and a coordinated response.

Teams must unite. Signals must be shared. And protection must shift from reactive to proactive.

Next, we break down what a modern cyberfraud attack looks like, including the types of attacks, how the attacker framework (also known as the cyberfraud kill chain) operates, and how AI is applied at every step to evade detection and scale operations.

Viewing the world through the eyes of the attacker

To build an effective defense, you have to think like the adversary.

Modern fraudsters no longer rely on isolated tactics. They run sophisticated campaigns that mimic legitimate behavior, evolve with each failed attempt, and exploit every gap in the user journey. And now, they use AI as a force multiplier.

Let's look at how modern cyberfraud attacks have evolved, and how AI now enhances every attack type and stage of the kill chain.

The types of cyberfraud

Today's attackers use a combination of bots, automation, AI, and readily available off-the-shelf tools to launch campaigns that are faster, smarter, and cheaper than ever before. Fraud-as-a-Service marketplaces, CAPTCHA-solving farms, cheap proxy networks, and open-source attack kits have lowered the barrier to entry for sophisticated fraud.

But the biggest shift is the rise of attacker-built AI agents. Unlike single-action bots, these agents operate with multi-step autonomy, tasked with carrying out a full sequence of events, such as scraping data, using that data to create fake accounts, and then making fraudulent purchases. They adapt in real time, make independent decisions across multiple requests, and mimic human behavior so well that they blend into legitimate traffic.

For leaders, the takeaway is clear: you can't afford to think of these modern fraud types in silos. They're often connected in practice, unfolding as part of larger, continuous attack chains that probe every weakness in your defenses. The types of fraud themselves haven't changed: fraudsters still seek to steal cre[illegible] [illegible]

Download the full guide to unlock the rest

But *how* they execute these attacks has evolved dramatically. Understanding each type and how attackers' tactics, techniques, and procedures (TTPs) have advanced is critical to building effective protection.

Account takeover (ATO) & credential stuffing

Automated bots test stolen credentials at a massive scale to gain unauthorized access to user accounts. Once inside, attackers can steal data, drain stored value, or use accounts as launch pads for broader fraud.

What's different today:

Attackers use AI to rotate IP addresses, mimic devices, and switch identity artifacts to bypass rate limits and detection. ATO is often the first domino in larger fraud schemes, leading to payment fraud, loyalty fraud, and more.

Fake account creation

Automated signups fuel abuses from promo code exploitation and spam to influence fraud and money laundering.

What's different today:

AI-generated identities and synthetic behaviors make fake accounts nearly indistinguishable from real ones. Bot operators can create tens of thousands within minutes, overwhelming systems that rely on manual review or static identity checks.

Card cracking

Bots test stolen or fabricated card numbers to identify valid combinations that can be monetized. These often lead to financial loss, chargebacks, and operational strain.

What's different today:

Attackers use AI and bots to optimize card testing sequences and avoid detection, often hiding behind residential proxies and mobile user agents. Once validated, cracked cards are quickly

Payment fraud

Fraudsters use stolen or forged payment details to make unauthorized purchases or drain user accounts.

What's different today:

Bots are increasingly used to initiate fraudulent transactions at scale, overwhelming fraud decision engines and inflating both chargebacks and false declines. As Gartner notes[4], "component technologies are still deployed and managed individually, resulting in data silos that necessitate information sharing and ingesting between systems. These disconnects and gaps between systems, teams and processes hinder cohesive defense strategies." Without shared signals across identity, transaction, and behavioral data, organizations struggle to distinguish legitimate activity from automated abuse, leading to missed fraud and unnecessary customer friction.

Ad fraud

Fake clicks, impressions, and conversions drain marketing budgets and distort campaign metrics.

What's different today:

Bots simulate full user journeys, including ad views, scrolling, click-throughs, and even form fills, creating patterns that blend seamlessly with legitimate traffic.

Scalping & inventory fraud

Bots target high-demand products like sneakers, concert tickets, and gaming consoles, buying inventory in bulk for resale at inflated prices.

What's different today:

Attacks are now multi-stage, using real-time product monitoring, fake accounts for purchases, and AI algorithms to time their execution precisely.

Download the full guide to unlock the rest

Scraping, data, & content theft

Bots and LLM-driven tools extract pricing, inventory, and other proprietary data, driving up operational costs and giving competitors and fraudsters an unfair advantage.

What's different today:

Advanced bots deploy evasion tactics such as dynamic mouse movement, browser spoofing, and cookie management to appear human and avoid detection. LLM crawlers steal content, resulting in less traffic from genuine users.

API abuse

Fraudsters exploit API endpoints to probe for vulnerabilities, exfiltrate data, or exploit business logic flaws.

What's different today:

Bots chain API calls to simulate entire user sessions, targeting gaps in authentication, pricing, or promo eligibility. APIs have become a prime attack surface for systematic fraud and data theft.

Layer 7 DDoS & application attacks

High-volume bot traffic floods applications and infrastructure, degrading performance or taking systems offline.

What's different today:

DDoS is increasingly blended with fraud operations, often used as a distraction while attackers execute payment theft, credential stuffing, or ATO attempts under the cover of chaos.

Friendly fraud

Customers dispute legitimate charges or exploit refund policies to receive products or services without paying, resulting in financial loss and chargeback fees.

What's different today:

Coordinated guides, fraud forums, and even templates created with generative AI now help fraudsters craft more convincing claims, making friendly fraud harder to detect and refute.

Download the full guide to unlock the rest

Promotion, loyalty, & refund abuse

Fraudsters exploit promotions, create multiple fake accounts to drain discount codes, abuse refund systems, or steal loyalty points.

What's different today:

Bots and automation enable these abuses at scale, with AI-driven scripts that detect new promos, generate synthetic users, and trigger refund workflows with plausible human-like behavior.

Cyberfraud attacker framework: How cybercriminals operate

Cyberfraud attacks aren't random.

They follow a structured, repeatable pattern that today's attackers have refined through automation, AI,

and human-in-the-loop orchestration. Understanding this pattern isn't just an academic exercise. It's the foundation of an effective defense.

Each phase of the attack chain represents a window of opportunity: a place where defenders can disrupt the attacker's plans, cut off access, and prevent downstream damage. But seizing those opportunities requires mapping your detection and response capabilities to the attacker's process, connecting security, fraud, and operational teams so they're watching the right signals at the right moments and speed.

CISOs and security executives must think like attackers, orchestrating their defenses around the attacker's predictable phases: reconnaissance, automation, account takeover, fraud execution, evasion, and monetization. Effective cyberfraud protection means staying one step ahead to anticipate attackers' moves, shut them down early, and close off paths before they're exploited. The strongest defenses also feed those insights back into the system, continuously sharpening detection and response over time.

Below, we break down the phases of the modern attack chain and where in the journey cyberfraud protection can shut them down.

We'll also highlight how AI is being leveraged at every stage, allowing fraudsters to operate at greater speeds and scale while avoiding detection.

Attacker framework

Cyberfraud attack chain

Stage	Activities	Disruption points
Reconnaissance	**Goal:** Identify vulnerable targets › Target identification with emphasis on high-value targets › Infrastructure fingerprinting with collection of login flows, checkout processes, and API endpoints › Identification of existing security/fraud controls such as WAF, CAPTCHA, 2FA, and [illegible] › Defense testing for error codes and threshold limits	**Mitigation approach:** Cyberfraud protection must block reconnaissance activities before attackers can map the environment or prepare targeted attacks › Deploy bot management to block scraping and unwanted bot and agents from crawling/probing › Use client-side challenges to deter scrapers › Monitor and alert on abnormal traffic patterns or user behavior [illegible]
Automation attacks	**Goal:** Attempt to gain access to user accounts › Credential stuffing › Identity testing › Fake account creation	**Mitigation approach:** Disrupt the automation process to make it more costly for fraudsters › Use client-side challenges to deter scrapers › Utilize identity verification during account creation, such as email or phone verification › Implement progressive Customer Identity and Access Management (CIAM) friction for anomalous traffic/requests (2FA or other step-up authentication) › Check email domain and IP reputation data

Stage	Activities	Disruption points
Account takeover (ATO)	**Goal:** Seize account control for fraud › Change passwords and account details, e.g., shipping address › Steal stored value like loyalty points, funds, saved card info, PII, etc.	**Mitigation approach:** Detect anomalous behavior and account activity › Implement Identity Threat Detection and Response (ITDR) tools › Monitor for account behavior deviations (e.g., shipping address changes, login IP shifts) › Require MFA › Monitor registrations and login events › Real-time session analysis to detect suspicious patterns
Fraud execution	**Goal:** Transaction execution & theft › Use stolen cards or saved payment info › Abuse promotions, discounts, and refund policy › Carding: testing multiple small transactions to test the card	**Mitigation approach:** Implement AI-powered account monitoring and protection › Require step-up multi-factor authentication › Baseline and compare interactions over time for anomalous behavior › Monitor and flag abnormal geographical patterns › Correlate a high number of events from an IP

Stage	Activities	Disruption points
Evasion	**Goal:** Maintain access and avoid detection › Utilize AI to mimic customer behavior (e.g., mouse movement/ clicks) › Rotate IPs, user agents, devices, and session behavior	**Mitigation approach:** Prevent prolonged access and detect obfuscation techniques › Continuously evolve bot detection logic using AI feedback loops and collective intelligence › Ongoing enforcement of protection policies (e.g., detail change alerts, session resets after high-risk events) › Correlation analysis of known compromised accounts
Monetization and exit	**Goal:** Convert to profit before detection › Resell of stolen or purchased goods (e.g., shoes, GPUs) › Sell account access or stolen data on the dark web › Launder funds	**Mitigation approach:** Trace and [illegible] to minimize damage & reduce incentives to continue fraud › Integrate with payment fraud platforms for alerts and account hold capabilities › Track and investigate downstream indicators of fraud, such as unusual shipping destinations and teleportation › Work with external partners to flag stolen goods listings on resale platforms

A new approach to defense: Cyberfraud fusion

The traditional divide between cybersecurity and fraud prevention no longer reflects the needs of businesses against modern threats. Attackers don't distinguish between exploiting systems and exploiting customers, but instead blend both into seamless campaigns. To respond effectively, organizations need a new approach: one that unifies cybersecurity and fraud functions, breaks down silos, and focuses on stopping attacks across the entire user journey, not just at isolated moments. Defenses must be continuous, connected, and built around the way attackers operate.

As privacy regulations tighten and identity signals become less reliable, detection strategies must shift from verifying who the user is to understanding what they intend to do. To stay ahead, organizations must shift from point solutions and siloed responses to a unified, intent-based strategy. One that connects identity, behavior, and context to detect not just what is happening, but why.

Download the full guide to unlock the rest

The need for intent-based detection in the AI era

Most cyberfraud doesn't begin at checkout. It starts much earlier, during reconnaissance, scraping, credential testing, or the creation of fake accounts. These precursor behaviors often go unnoticed until real damage is done. By the time payment fraud or account takeover is detected, the attackers may have already achieved their objectives.

A new, proactive approach begins with detecting intent.

Instead of simply asking "Is this a bot?" or "Is this user known?", modern defenses analyze every request in real time to understand intent: what is this user trying to do? This shift from identity to intent is the difference between reacting after fraud has occurred and stopping it before it happens.

This is even more paramount given the rise of agentic AI, both in its use by genuine users and by fraudsters. Intent-based detection, powered by machine learning and behavioral analysis, enables companies to

differentiate between AI agents conducting legitimate tasks, such as price comparison or transaction assistance, and those engaged in malicious activities, like scraping, fraud, or credential stuffing.

This shift from chatbots to agentic AI mirrors the transition from browser-based traffic to mobile apps some years back. Just as businesses had to rethink web security when mobile apps changed how users interacted with their services, they must now adapt to AI agents.

Organizational structure: Aligning to the attacker's framework

Attackers move fluidly across credential stuffing, fake account creation, ATO, payment fraud, and pr[illegible] organizations still rely on legacy structures where cybersecurity, fraud, and business operations teams work in silos, each managing their own tools and signals, without any shared telemetry.

This outdated model creates blind spots that attackers exploit. Leaders like CISOs, Chief Risk Officers, and VPs of Trust & Safety are shifting away from these fragmented structures. Much like adoption of DevOps methodology broke down the wall between development and IT to accelerate delivery, **cyberfraud fusion** offers the potential to break down the barrier between fraud and security to align teams and workflows around the attack.

Bringing together key functions

At their core, cybersecurity and fraud teams share the same ultimate mission: stopping malicious actors and automation before they can disrupt operations, steal value and data, and erode trust.

Effective cyberfraud protection depends on tight coordination between cybersecurity, business operations, engineering, and fraud prevention teams.

Discipline	Primary focus
Cybersecurity	Protects systems, applications, and data from malicious access and exploitation. Key areas include bot mitigation, API security, DDoS defense, WAF management, threat detection, incident response, and infrastructure hardening
Business operations	Cross-functional team that deploys and operates the business apps/APIs. Team members include representatives focused on front and back end systems, CIAM, API management, app delivery infrastructure, and site reliability (SREs).
Fraud prevention and operations	Focuses on detecting and preventing financial and behavioral abuse. Core functions include transaction fraud detection, account takeover (ATO) prevention, fake account detection, promo abuse, refund fraud, loyalty program abuse, and chargeback management.

Cyberfraud protection

Download the full guide to unlock the rest

These functions can no longer operate in isolation

Effective protection depends on their ability to share signals, investigations, and joint threat models. When cybersecurity and fraud teams align around shared goals and collaborate with the business ops and engineering teams that own customer-facing systems, they can respond to threats holistically, with speed and precision that siloed teams can't match.

What fusion looks like in practice

Fusion, at its core, is about day-to-day collaboration. Here is what successful cyberfraud fusion looks like in practice.

- **Cross-functional teams** made up of SOC analysts, fraud investigators, engineers, and data scientists collaborate on the same threats, mirroring how attackers operate across technical and financial surfaces.
- **Shared dashboards and unified case management** ensure everyone works from the same data, eliminating duplicate investigations and gaps in context.
- **Aligned leadership and KPIs** bring fraud and security under the same executive (often the CISO) to drive coordinated priorities, tooling, and response.
- **Real-time, AI-powered protection** assesses behavior and intent across the user journey, not just identity at the point of login or checkout.
- **Global collaboration** [illegible] benefiting from a broader network of insight.

Download the full guide to unlock the rest

Across industries, forward-looking organizations are already converging cybersecurity and fraud operations.

Banking & traditional financial institutions are increasingly aligning cybersecurity and fraud teams under a shared leadership structure, often reporting into a Chief Risk Officer or a combined Security & Fraud division. This shift enables SOC analysts and fraud investigators to collaborate on shared signals like credential compromise and suspicious transaction behavior, reducing time to detection.

E-commerce & retail companies are forming cross-functional cyberfraud units that bring together bot mitigation, account protection, and abuse prevention under the CISO or a VP of Trust & Safety. This structure streamlines responses to attacks that span login, checkout, and loyalty systems.

Fintech organizations, especially those in high-regulation markets, are merging security, fraud, and compliance teams into centralized risk operations. In many cases, both cybersecurity and fraud prevention now report to the same executive, helping the business stay ahead of threats that target infrastructure and financial flows simultaneously.

A modern organizational reporting structure for a company that has adopted cyberfraud fusion.

Why legacy fraud tools can't keep up

Legacy fraud prevention tools were built for a different era when attacks were slower, simpler, and largely human-driven. Back then, static rules, spreadsheets, and reactive manual review were enough. But today's attacks move at machine speed, combining bots, AI, synthetic identities, and real-time evasion tactics that overwhelm these older approaches.

Even tools that layer AI onto traditional identity checks fall short. That's because identity alone doesn't reveal intent. Fraudsters now use verified devices, clean credentials, and human-like interaction patterns to blend in. Meanwhile, stricter privacy regulations are further weakening fraud prevention by restricting the collection of customer data that helps verify user identity, making identity-based detection even less effective. Traditional fraud tools are built and deployed to inspect signals at intervals in the user journey. Tools that don't inspect 100% of user requests in real time often miss early-stage or session-warming threats, like reconnaissance and automated attacks, making it harder to stop fraud before it starts.

The result?

Higher false positives, more missed threats, higher fraud costs, and a widening gap between attacker sophistication and defender capabilities.

Cyberfraud protection: Core solutions, capabilities, & platform selection

As cyberfraud grows more advanced, the tools to fight it must evolve too. Point solutions and reactive tools can't keep up with sophisticated, AI-powered threats that span login, checkout, APIs, and everything in between. Next, we break down the landscape of cyberfraud protection, including the tools that form its foundation, and a maturity model to help benchmark your organization's current maturity level.

The solutions that make up cyberfraud protection

The growing category of cyberfraud protection spans multiple solution types today, each focused on parts of the problem.

Download the full guide to unlock the rest

Solution category	Examples
CDN, cloud, and network security providers	Network edge attack filtering, attack surface management, threat intelligence
Specialized bot management vendors	Advanced detection for automated attacks
Web and API security	Protection against App/API abuse, credential harvesting, business logic defenses
Payment fraud specialists	In session transaction monitoring and intelligence, chargeback reduction, fraud decisioning
CIAM - ID verification & KYC tools	Identity confirmation and authorization for users

Individually, each tool addresses a specific part of the problem. **Together, they form true cyberfraud protection.**

The cyberfraud protection maturity model

Organizations don't transform their cyberfraud defenses overnight.
The journey from basic to proactive protection follows a maturity curve defined by how teams detect, share, and act on signals across the user journey, as well as the tools they have in place to defend against modern-day threats.

Cyberfraud protection maturity model

Maturity	Characteristics	Teams	Tooling/Protections
Basic	Reliant on common controls centrally provided dedicated to specifically addressing cyberfraud	IT/Tech/DevOps	Use of IT common controls with manual and • CIAM • Network security • WAF and basic bot (rules and signatures)
Reactive	Separate controls are implemented at the department level	Separate IT, security, business ops, and fraud teams	Adjacent "check-the-box" tooling. Everything in the previous row, plus: • Advanced WAAP • Specialized bot management • Risk-based step-up authentication integration with CIAM • Chargeback management platforms

Download the full guide to unlock the rest

Maturity	Characteristics	Teams	Tooling/Protections
Tactical	Collaboration between teams using point solutions to monitor and respond to threats at each stage of the attack framework	Separate security and fraud teams. Workflow processes are created among representative teams to share independent threat and risk data and analytics	Dedicated point solutions. Everything in previous rows, plus: › Full-stack bot management and fraud protection platforms › Know your customer (KYC) tools › Real-time behavioral analytics and intent modeling
Proactive	Threats anticipated, automated and integrated defenses, insights driving actions/strategy	Unified Cyberfraud Fusion team	Unified tooling processes and team. Everything in previous rows, plus: › Shared and integrated dashboards, tools, and data for fraud and [illegible] teams. Teams have shared signals and detection engines.

The cyberfraud protection maturity model at-a-glance

Basic: Common controls

At this stage, organizations have implemented foundational common controls designed to block unsophisticated automated threats that could lead to cyberfraud. Businesses rely on common, organization-wide protections typically managed by centralized IT teams. These include web application firewalls (WAFs), basic bot filters, network firewalls, and customer identity and access management (CIAM) systems.

Often integrated into CDN or service provider offerings, these common controls provide broad coverage across the domain but are not tailored to specific customer-facing functions like login or checkout pages. There are no dedicated cyberfraud detection capabilities in place, and any fraud reviews are manual and conducted after the fact.

Protection at this stage:

- WAF, firewall, and basic traffic filtering
- [illegible]
- Basic bot protection (e.g., signature-based detection) and CAPTCHA
- Manual, post-event fraud review processes

Reactive: Disparate point controls

As threats grow more complex, organizations bolt on more tools: separate platforms for bot mitigation, payment fraud, account takeover protection, and content abuse monitoring. Cybersecurity and fraud teams operate independently, using different solutions with little data sharing. Investigations are slow, and attackers slip through the cracks between siloed defenses.

Additional protection at this stage:

- Advanced Web Application and API protection (WAAP)
- Specialized, AI-powered bot management and anomaly detection

- Payment fraud detection/transaction monitoring rule enforcement solutions
- CIAM with risk-based step-up MFA
- Chargeback management platforms

Tactical: Tailored controls and tools

At this stage, organizations recognize the limitations of fragmented, reactive controls and begin aligning cybersecurity and fraud detection workflows. AI-driven detection models help surface anomalies earlier, enabling faster, more dynamic responses to threats before fraud is completed. Security and fraud teams have started sharing threat signals to correlate suspicious user behavior, block coordinated attacks sooner, and reduce the time needed for investigation.

Ad

Download the full guide to unlock the rest

- Full-stack bot management and fraud protection platforms
- Real-time behavioral analytics and intent modeling
- Know your customer (KYC) tools for improved identity verification, risk scoring, transaction analytics, and case management integration

Proactive: Full cyberfraud fusion nirvana

The most advanced organizations don't just integrate tools. They unify teams, data, and decision-making under a shared cyberfraud protection strategy. Security, fraud, and operations teams operate as one function, reporting to a common C-suite leader, such as a CISO.

Real-time, intent-based decision-making becomes the standard. AI autonomously detects and blocks threats at the earliest signals, before a bot with bad intent even lands on your website, or a fake account is created, or an account is compromised. DDoS protections add another critical layer, mitigating volumetric

and application-layer attacks that are often used as distractions to mask fraud operations, ensuring system availability even during high-risk, high-traffic events.

At this level, protection is proactive, autonomous, and AI-driven.

Additional protection at this stage:

- Unified fraud and cyber defense platforms powered by multi-layered, real-time AI
- Edge-based intent detection and mitigation
- Autonomous decision-making across web, app, and API surfaces

Organizations that fully leverage an integrated cyberfraud protection platform reach the highest level of cyberfraud defense maturity.

They combine real-time behavioral signals, advanced anomaly detection, and edge-level mitigation to protect every surface, from account flows and digital ecosystems to APIs, payment endpoints, and infrastructure. With coverage spanning bot attacks, malicious AI agents, DDoS threats, compliance risk, and fraud abuse, this unified approach stops threats before they impact users, systems, or revenue.

Download the full guide to unlock the rest

The future of cyberfraud protection: AI-driven, real-time, & built to adapt

Today's attacks move fast, blend tactics, and evolve constantly.

Stopping them requires real-time, adaptive protection that understands intent and responds instantly.

AI is central to this shift, but not just any AI. Protection must be multi-layered, continuously learning with closed feedback loops and collective intelligence, and deployed where it matters most: at the edge.

Here's what's next:

Multi-layered AI becomes foundational: Behavioral analysis, anomaly detection, threat scoring, and response modeling will no longer be optional add-ons; they will be foundational. Stopping fraud requires AI that correlates signals across every stage of the user journey and updates dynamically with each new interaction.

Real-time adaptation across all traffic: Batch updates can't keep up. Protection must happen, in milliseconds, across web, mobile, and APIs. The future is real-time decisioning that scales across billions of requests while minimizing friction for real users.

Expansion to emerging fraud surfaces: As traditional checkpoints harden, attackers shift focus. Expect more fraud targeting loyalty programs, refund systems, embedded finance APIs, and AI agents. Defenses must extend beyond login and checkout to every touchpoint where value can be extracted.

AI-on-AI defense: Fraudsters are building agents that act independently, mimic human workflows, and make decisions mid-session. Countering them requires equally adaptive defenders: AI systems that can detect intent shifts, interrupt agent behavior, and identify synthetic activity as it unfolds.

Shared intelligence at scale: An isolated view is a limited one. Leading platforms will draw on collective intelligence from across their networks to detect emerging threats earlier and apply those insights to protect every customer in real time.

This is where cyberfraud protection is headed, and why choosing the right platform matters.

Choosing the right cyberfraud protection platform

No single platform solves everything. The question is which one is built to adapt fast enough and intelligently enough to meet tomorrow's threats.

It's not just about current capabilities, but whether the vendor is committed to a comprehensive cyberfraud protection strategy: one that prioritizes cross-functional defense, real-time detection that leverages multi-layered AI, and continuous innovation. Look for a partner who delivers value now and has a clear roadmap aligned with where your business (and the fraud landscape) is headed.

Why DataDome is leading the future of cyberfraud protection

DataDome was built with a single mission: to free the web from fraudulent traffic.

Our Cyberfraud Protection Platform stops today's most advanced threats using real-time, multi-layered AI that protects every step of the user journey without compromising performance or user experience.

Real-time AI, built for scale

We analyze 100% of requests in under 2 milliseconds, using AI that learns from over 5 trillion signals per day to detect and adapt in real time.

Protection that outperforms

Our <0.01% false positive rate leads the industry, ensuring legitimate users aren't blocked even as attacks evolve.

Download the full guide to unlock the rest

Full-journey coverage

From first interaction to final transaction, we protect web, mobile, and APIs, stopping bots, fake accounts, scraping, payment fraud, AI fraud, and more.

Built for both security and fraud teams

Shared signals, unified workflows, and real-time collaboration help cross-functional teams respond faster and work smarter.

Intent-based detection

In the era of agentic AI, it's no longer just about detecting bots or humans: it's about understanding intent. Our platform evaluates behavioral patterns across the user journey to distinguish between legitimate and malicious intent in real time.

Download the full guide to unlock the rest

DataDome's Cyberfraud Protection Platform continuously discovers, detects, analyzes, and protects your entire digital footprint—across websites, mobile apps, and APIs.

It starts with automatic discovery of unprotected assets to eliminate blind spots before fraud happens. Every request is then analyzed in real time using thousands of AI models trained on over 5 trillion signals daily, ensuring unmatched detection accuracy. Protection policies operate on autopilot across your stack, defending against bots, account fraud, DDoS attacks, and more. Actionable dashboards and deep threat analytics provide the insights you need to stay ahead—making cyberfraud protection seamless, proactive, and precise.

DataDome

Recognized as a Leader in the 2024 Forrester Wave™ for Bot Management

Trusted by over 300 leading brands worldwide

Etsy

The New York Times

SOUNDCLOUD

ASUS

Tripadvisor

petco

PayPal

Stopping cyberfraud before it happens

AI is changing everything.

Fraudsters now launch AI-powered attacks that adapt in real time, blending bots, deception, and automation to exploit every surface. At the same time, everyday users are adopting AI agents to browse, shop, and transact. The landscape is shifting fast, and defenses built around static rules and siloed teams are falling behind.

Staying ahead means rethinking the entire defense stack. It means collapsing the divide between cybersecurity and fraud, aligning teams, and introducing a new first line of defense: real-time, intent-based detection that identifies [illegible] multiple lines of defense remain critical, but the organizations that will thrive are the ones that act early by sharing signals, adapting in real time, and using AI not just to detect, but to stop attacks before they start.

No more silos. No more static defenses. Just protection that outperforms before fraud ever has a chance to walk through the door.

See where you stand

Take the free Vulnerability Scan or request a demo to see the Cyberfraud Protection Platform in action.

Download the full guide to unlock the rest

datadome.co