



Protect Your Business and Customers from Online Fraud

Online fraud has recently skyrocketed, with fraudsters adapting and escalating to take advantage of major shifts in the digital landscape. Automated and manual, human-driven fraud can jeopardize strategic business outcomes and inflict massive losses for both company and consumer. But despite the demand for digital services and the growing risk for fraud, customers also expect a frictionless experience, making online fraud protection a difficult balance.

Consumers lost \$5.8B to fraud last year – up 70% over 2020¹

Spurring Online Fraud Growth



Increase in permanent work-from-home and remote users



Acceleration of digital channels without proper security



Silos between fraud and security teams stalling prevention



Adapting fraudsters capitalizing on advanced technology at scale

2021 data has shown criminals will change strategies to evade detection and maximize the amount of information they can extract from victims²

Deter Online Fraud with a Holistic and Unified Approach

Business leaders face a tough choice: implement layers of security to verify human behavior and identity, potentially frustrating users, or accept fraud losses. The F5 solutions for online fraud prevention include an AI system trained on verified human data that evaluates truth and intent to help stop fraud in real time.

By 2023, addressing policy abuse will become an essential requirement in 50% of RFPs for online fraud detection in digital commerce, up from less than 10% in 2021³

F5 and Google Cloud can help you:

Bot Defense

Maintain efficacy as attackers retool their targets and techniques

Authentication Intelligence

Securely reduce friction to improve customer experience and maximize revenue

Account Protection

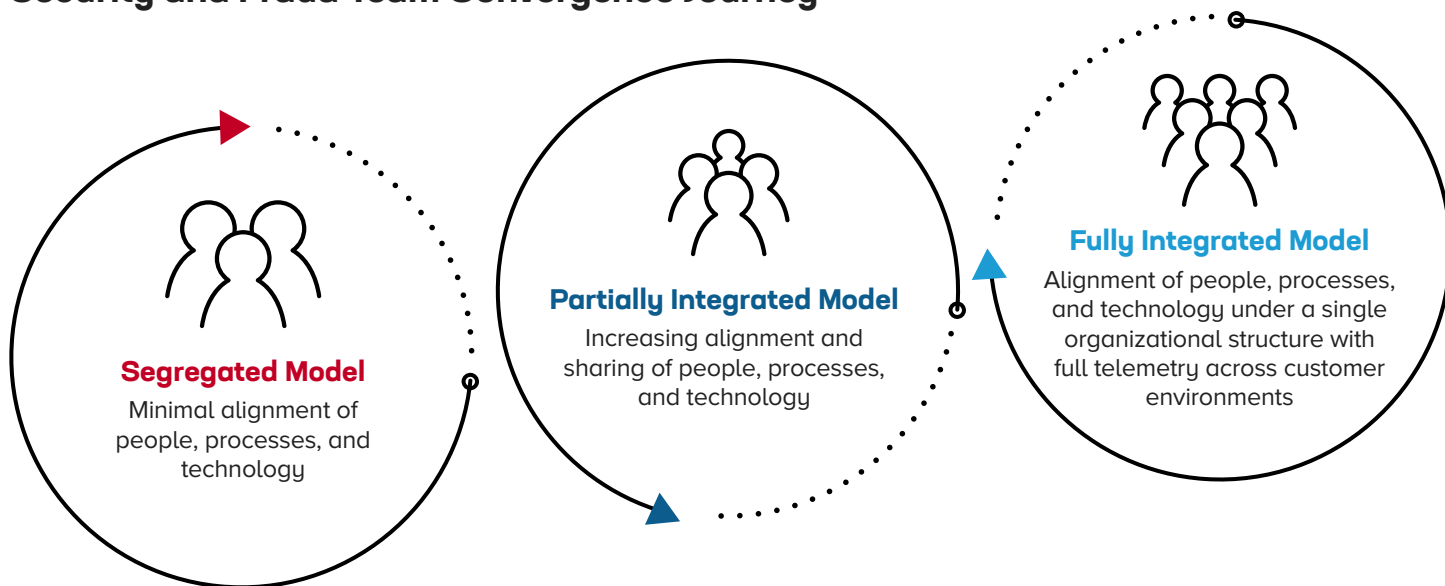
Monitor application transactions for truth and intention to prevent fraud



The Convergence of Security and Fraud Teams

Integrating security and fraud teams is the best weapon against financial crime. Increased collaboration improves risk management and customer outcomes. By establishing an integrated model and fusion center between security and fraud teams, organizations can create an ecosystem of shared tools with proactive and preventative intelligence that mitigates financial crime and allows customers to transact seamlessly. This strategy of synergy has numerous tactical and cultural challenges but is a critical investment to compete in a dynamic, digital business climate.

Security and Fraud Team Convergence Journey



Prevent Online Fraud with a Multifaceted Approach

Prevent Account Takeover

Stop account takeover (ATO) before it leads to fraud, lost revenue, and damage to customer loyalty.

ATO is often the precursor to fraud. To effectively mitigate ATO and the widespread business impacts to revenue, operations, and brand, deploy security that stays resilient no matter how attackers try to exploit your technology, people, or processes—without friction that frustrates your customers.



ATO losses increased 90% in 2021 as criminals hijacked victims' online lives⁴

Stop Human-Driven Fraud

Prevent fraud in real time without impacting the user experience.

For enough value, attackers will bypass anti-automation controls with manual fraud. F5 solutions evaluate truth and intent to prevent fraud in real time—without impacting the user experience—thereby improving top-line potential while reducing bottom-line pressure.



Mitigate Bots and Abuse

Deter attackers that use malicious automation to commit account takeover and fraud.

Just as enterprises adopt automation to gain process efficiencies, attackers have embraced bots and automation to scale their attacks, bypass security countermeasures, and compromise customer accounts. F5 solutions automatically adapt to changing attack tactics without inserting user friction, ensuring business success and customer satisfaction.



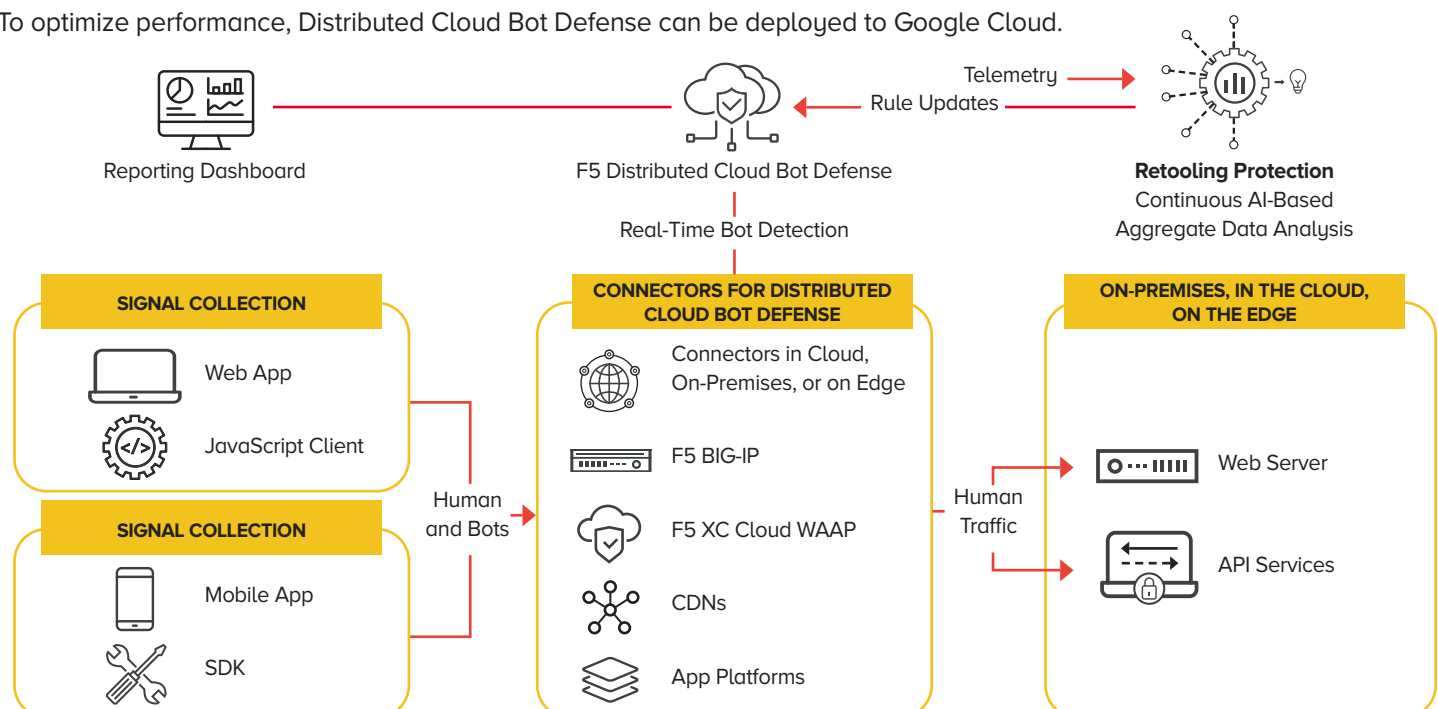
73% of businesses face weekly bot-based attacks⁵

F5 Solutions for Online Fraud Prevention

F5 Distributed Cloud Bot Defense

Bot attacks are difficult to stop—criminals retool to bypass defenses, rapidly solving CAPTCHAs and mimicking human behavior. To stay ahead of bots, Distributed Cloud Bot Defense uses AI to achieve unparalleled long-term efficacy and zero customer friction. Distributed Cloud Bot Defense protects against a broad set of bot-based attacks, including credential stuffing, account takeover, fraud, and account abuse.

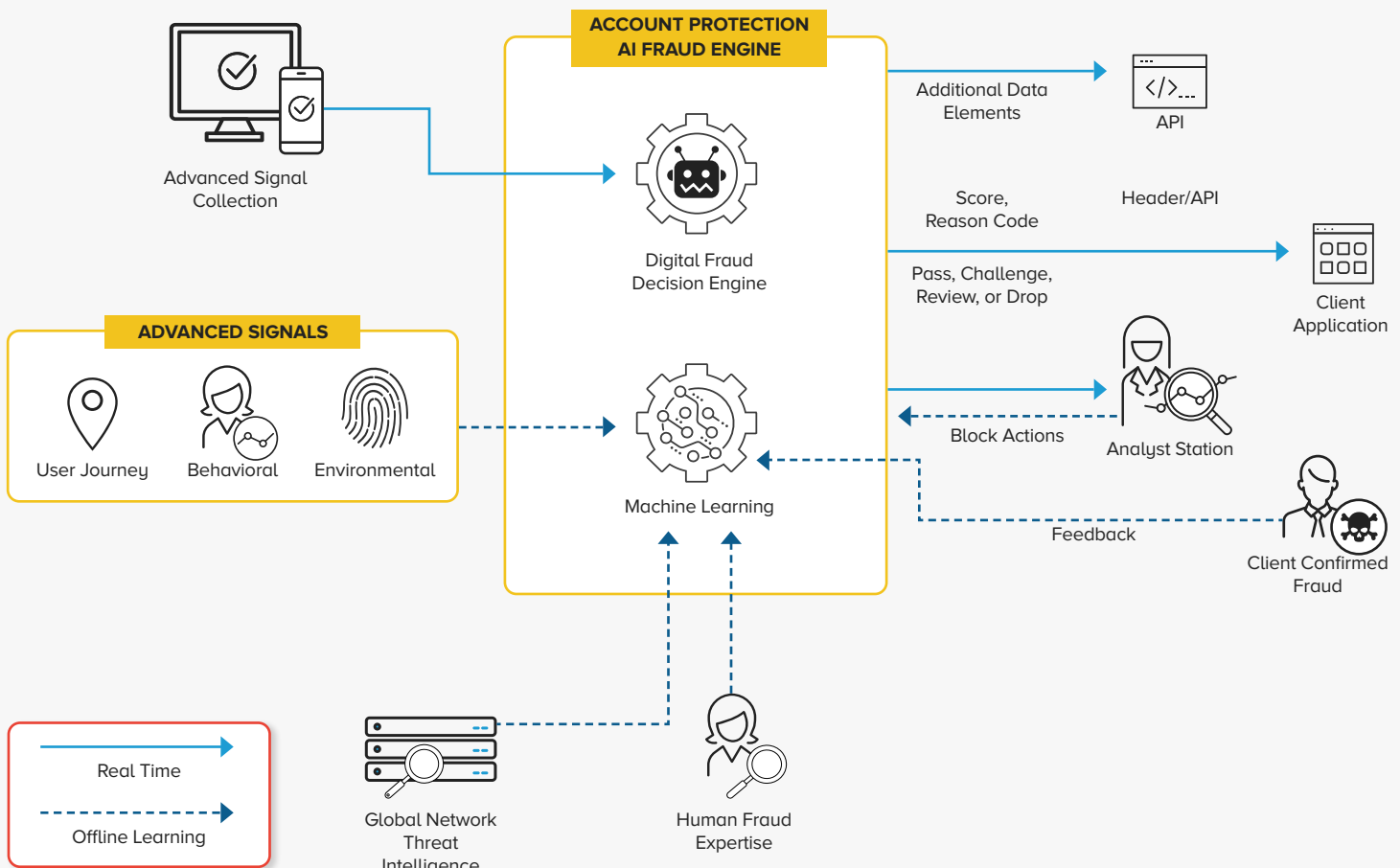
To optimize performance, Distributed Cloud Bot Defense can be deployed to Google Cloud.



F5 Distributed Cloud Account Protection

Fraud attacks and losses continue to increase. Organizations struggle to balance continuously retooled threats, pressure to reduce customer friction, surges in fraud cases to investigate, and staffing shortages. Distributed Cloud Account Protection provides application security and fraud protection powered by a real-time, closed-loop engine and large-scale unified telemetry to reduce customer friction and stop fraud before it happens. Distributed Cloud Account Protection blocks fraud missed by existing tools, slashes friction for legitimate consumers by up to 90%, and reduces workloads for fraud teams.

Slash friction for legitimate consumers by up to 90%



Google Cloud Is an Important Partner in Online Fraud Protection

Google Cloud is a more flexible, secure cloud provider that embraces open source, making it the best platform to migrate infrastructure and modernize applications. It's also the most multi-cloud-friendly, providing pioneering capabilities around Kubernetes as well as big data and analytics. Google Cloud has always prioritized security; the platform's strong security and cutting-edge encryption allow companies to safely store and analyze sensitive personally identifiable information.

Discover F5 solutions in the Google Cloud Marketplace or visit f5.com to learn more.

Sources:

1. FTC, "New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021," Feb 2022
2. Javelin, "2022 Identity Fraud Study: The Virtual Battleground," Mar 2022
3. Gartner, "Market Guide for Online Fraud Detection," July 2021
4. Javelin, "2022 Identity Fraud Study: The Virtual Battleground," Mar 2022
5. Barracuda, "Bot Attacks: Top Threats and Trends," Sept 2021

