Stop Online Fraud with F5 Distributed Cloud Account Protection

The most sophisticated attackers will retool and adapt against all countermeasures, using techniques that leverage human behavior to evade detection. Stopping targeted, human-driven fraud requires adaptive, real-time detection of fraudulent activity across the entire user journey—with no added friction.

KEY BENEFITS

Reduce fraud losses
Distributed Cloud Account Protection accurately identifies fraudulent activity in real time across the entire journey. Its AI fraud engine, fueled with advanced signal collection and highly trained machine learning (ML) models, detects malicious intent and stops fraud before it happens.

Increase operational efficiency
Distributed Cloud Account Protection delivers a single, high-fidelity outcome and blocks fraud in real time. There's no need to interpret scores or write or maintain rules—and transactions flagged for review are dramatically reduced. Additional outputs include reason codes and data elements to enhance existing client fraud detection systems.

Protect legitimate users
By accurately separating legitimate users from fraudsters, Distributed Cloud Account Protection enables a low-friction customer experience without burdensome MFA.

DISTRIBUTED CLOUD ACCOUNT PROTECTION LEVERAGES A UNIQUE SET OF DATA FROM EACH APPLICATION SESSION TO ACCURATELY DETERMINE IN REAL TIME IF USER INTENT IS MALICIOUS OR NOT.

As online activity increases and digital footprints expand, so too does the overall application attack surface. Attackers use powerful AI/ML frameworks, tools, and techniques to automate attacks and compromise customer accounts—leading to stolen personally identifiable information (PII), account takeover (ATO), and to increasing online fraud. Juniper Research estimates online fraud losses will exceed $48 billion per year by 2023.[1]

Continued fraud losses

In response to the changing threat landscape, and to combat increasingly sophisticated attackers, security and fraud teams have deployed an arsenal of anti-fraud solutions. Unfortunately, ATO fraud losses continue to rise, as sophisticated attackers defeat traditional fraud detection approaches.

Costly operational complexity

Layered fraud detection solutions create complex operations, causing stress, inefficiency, and high cost. Most of these solutions also require time-consuming tuning and maintenance, and often require multiple reviews due to high false positives rates.

Finding balance between protection and customer experience

Revenue is the top business priority—and it can be negatively affected by the friction that fraud controls create. Customers may lose patience or interest when countered with identity and authentication controls such as multi-factor authentication (MFA), knowledge-based authentication (KBA), CAPTCHA, and more.

Real-Time Fraud Detection with a Fully Managed Closed-Loop Solution

Reducing online fraud against web and mobile applications is difficult. Despite implementing numerous fraud tools, most enterprises still lose millions annually to fraud. Worse, fear of fraud also causes organizations to impose burdensome friction on legitimate users. F5® Distributed Cloud Account Protection (XC Account Protection) gives fraud teams a new and powerful solution to detect and eliminate online fraud, without compromising the user experience.

Block fraud, slash friction, and reduce fraud prevention team’s workload

Distributed Cloud Account Protection is a closed-loop engine that blocks fraud in real time. It detects and stops account takeover, malicious account creation, exploitation of stolen accounts, and other fraudulent activities. In production Fortune 500 environments, Distributed Cloud Account Protection identifies 2-5 times more fraud per month than current solutions, while maintaining false positives at pre-existing baseline levels.

DISTRIBUTED CLOUD ACCOUNT PROTECTION DELIVERS

Reduced fraud
2x fraud detection in many production environments

Less friction
Eliminates excess MFA challenges for legitimate users

Less effort
Reduces complexity and operational demands

Allow trusted customers to transact

Distributed Cloud Account Protection imposes less friction by reducing MFA challenges for legitimate users. Most B2C organizations unnecessarily issue thousands of MFA challenges to site visitors because legacy fraud tools fail at identifying good users from bad. Distributed Cloud Account Protection makes it much easier to reduce friction for legitimate users and increase friction for fraudsters.

Actively block fraud without writing or maintaining rules

Most fraud tools deliver raw data like device properties and risk scores, and expect organizations to use these organizations to use these to write and maintain complex rules. Distributed Cloud Account Protection allows customization to actively block, challenge or pass based on organizational risk tolerance in real time without the need to write or maintain rules. Distributed Cloud Account Protection also measures and reduces the number of transactions flagged for review and aims to drive this number down by 50% compared to prior baselines.

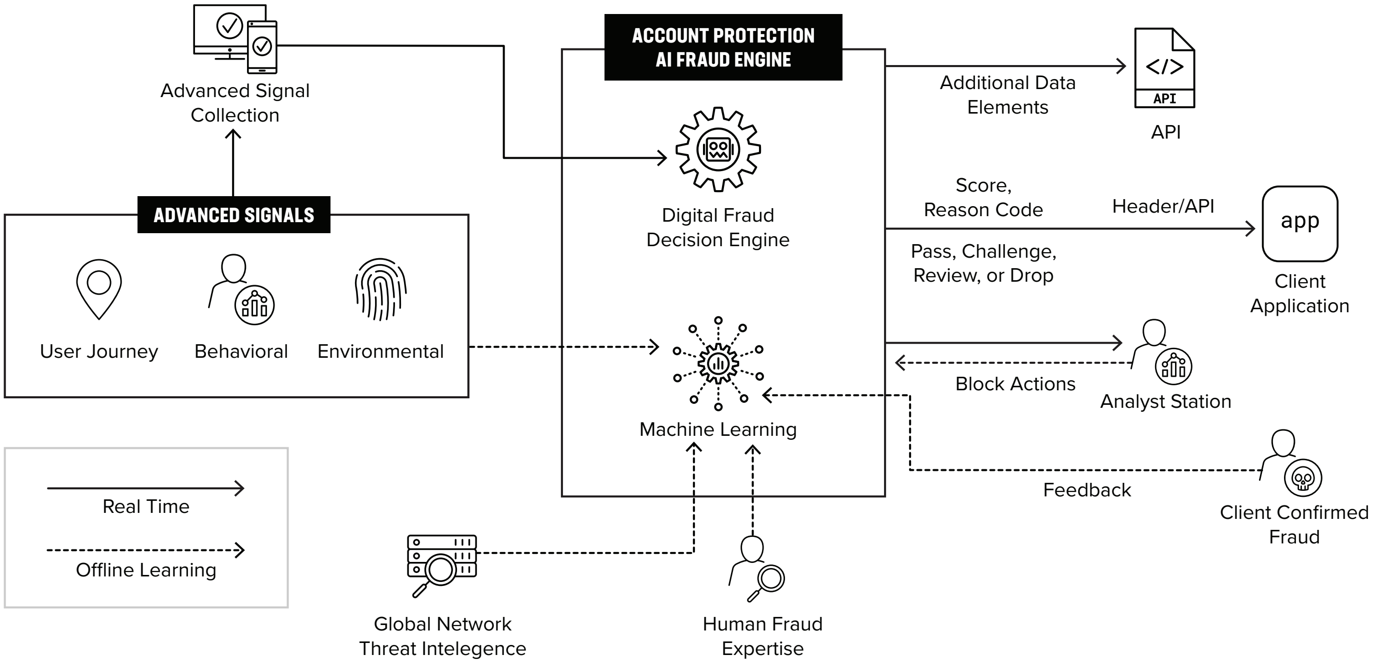

Figure 1: Distributed Cloud Account Protection is a cloud-managed service dedicated to stopping fraud across the user journey. A JavaScript tag collects client signals and securely communicates with an AI engine for real-time fraud decisions.

Understand visitor intent

Distributed Cloud Account Protection evaluates each online transaction across a set of telemetry, environmental, and behavioral biometric data, starting from the first time a visitor arrives at a protected web or mobile application, through to account creation or login, and continuing through all aspects of the user's journey. Distributed Cloud Account Protection can even connect context across different browsers and devices operated by the same user, and leverage insights from its global network of organizations to accurately determine user intent.

KEY FEATURES

Unified, secure telemetry
Determines user intent with advanced signal collection including user journey signals, behavioral and environmental insights, coupled with global network threat intelligence.

Real-time fraud decisions
Powered by unique telemetry and adaptive ML models, the Distributed Cloud Account Protection AI Fraud Engine delivers real-time fraud decisions (Pass, Challenge, Review or Drop), as well as additional data elements for integration with existing fraud detection systems.

Adaptive machine learning
Distributed Cloud Account Protection uses ML models to recognize fraud patterns and identify risky transactions, while minimizing false positives. Models are trained with insights from confirmed customer fraud files, telemetry, global threat intelligence, and human fraud expertise.

WHEN FRAUDSTERS CHANGE TACTICS (AND THEY WILL!), DISTRIBUTED CLOUD ACCOUNT PROTECTION AUTOMATICALLY ADAPTS.

Minimize friction with closed-loop AI

The advanced signals collected by Distributed Cloud Account Protection are analyzed and processed in real time by the powerful AI fraud engine, which also quickly adapts as fraudsters retool their attacks. The result is a single, high-fidelity, real-time outcome. Distributed Cloud Account Protection immediately reduces fraud, and delivers increasingly stronger fraud detection as the engine consumes more data. The result is more blocked fraud, fewer transactions that need investigation, and less friction for legitimate users. Distributed Cloud Account Protection also offers Scores, Reason Codes and additional data elements which can be consumed by existing client fraud detection systems.

Reduce investigation time and management burden

Distributed Cloud Account Protection is a closed-loop system that delivers fraud prevention Outcomes as a Service and relieves much of the investigation and management burden from fraud teams. Distributed Cloud Account Protection maintains and tunes the system, delivering real-time decisions to applications and an ever-decreasing number of incidents for fraud teams to investigate.

Conclusion

The digital-first economy has vastly increased the threat landscape. As businesses expand their digital footprint, so do fraudsters, who have easy access to sophisticated attack tools and can nimbly adapt with retooled schemes. Despite deploying a complex arsenal of point solutions, which stress teams and increase operational costs, fraud losses continue to rise.

Distributed Cloud Account Protection gives fraud teams an innovative solution to detect and eliminate online fraud. Powered by a closed-loop AI fraud engine, which evaluates each online transaction in real time across a set of telemetry, environmental, and behavioral analytics data, and leverages highly trained ML models, it focuses on understanding user intent. Distributed Cloud Account Protection delivers a single, high-fidelity, real-time outcome to client applications—increasing fraud detection, and reducing complexity and operational cost, while enhancing the customer experience.

To learn more, contact your F5 representative, or visit F5.com.

[1] Juniper Research Online Payment Fraud Market Report, found at https://www.juniperresearch.com/researchstore/fintech-payments/online-payment-fraud-research-report