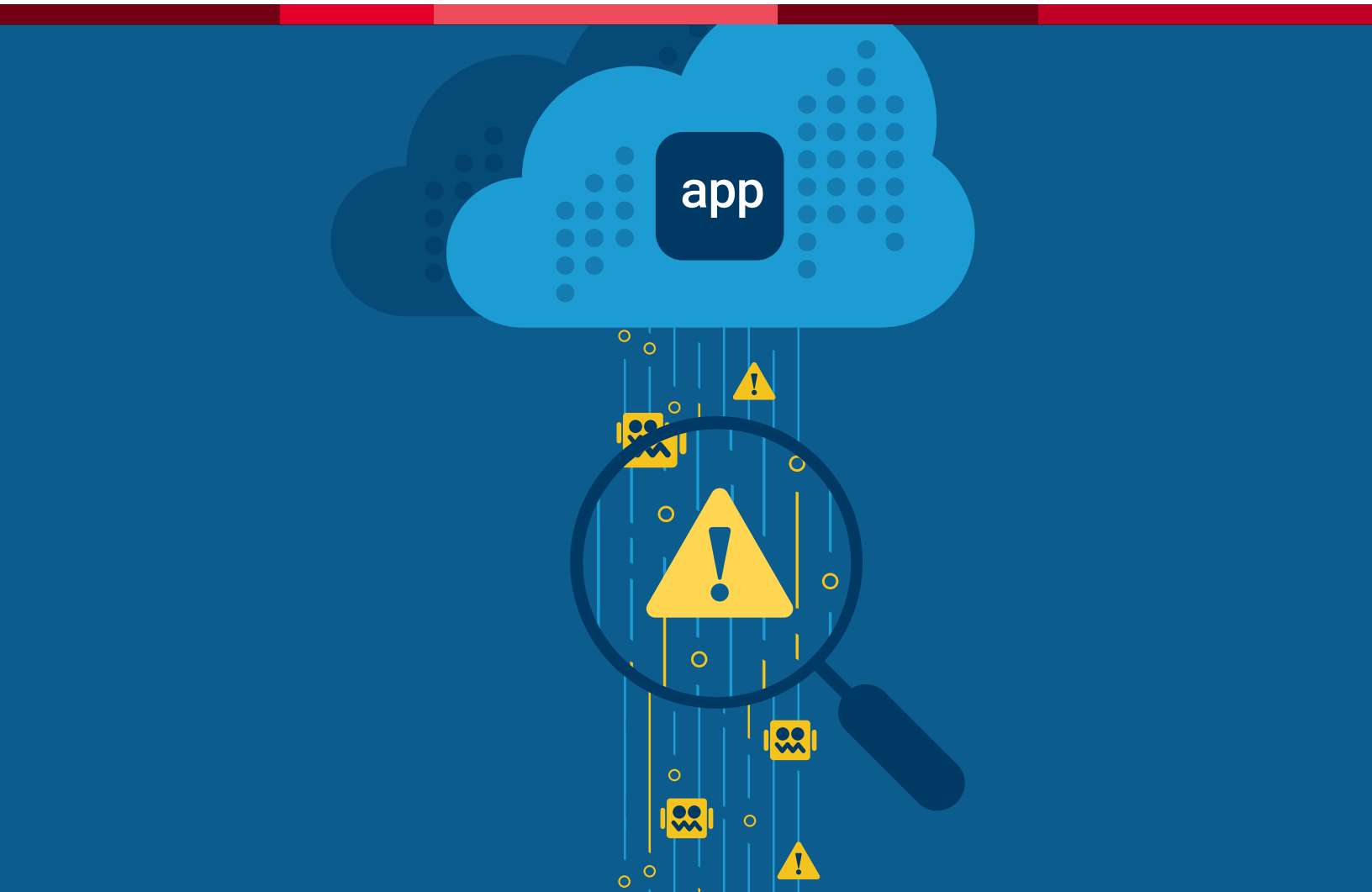
SOLUTION OVERVIEW

Detect More Fraud with Rich User Insights from F5 Distributed Cloud Data Intelligence



KEY BENEFITS

Detect fraud early in the user lifecycle
Access real-time telemetry signals to detect and mitigate malicious intent before harm is done. Prevent revenue losses and protect customers' confidential data.

Maximize fraud detection and fraud investments
Augment existing fraud systems with enriched telemetry gathered from users' interactions with your applications to better detect, confirm, and mitigate account takeover, account origination, and other attack methods.

Uncover digital identity risk
Gain a multi-dimensional view of identity risk, with actionable and contextualized user behavior, device identification, and network information gathered using rich telemetry signals.

Empower data-hungry security and fraud teams
Elevate your data science journey and bolster fraud detection capabilities with the essential intelligence required to detect suspicious patterns.

IMPROVED TELEMETRY EMPOWERS BETTER FRAUD DETECTION AND GREATER REVENUE PROTECTION.

Access rich user behavior, device identification, and network data intelligence to detect, confirm, and mitigate manual fraud activities previously invisible to fraud detection systems and tools already in place.

Ingest contextualized signals and intelligence into your existing fraud tools and systems to more effectively detect and thwart account takeovers, fraudulent account openings, and other instances of fraudulent behavior in real-time.

Unmask More Fraud with Rich User Behavior, Device, and Network Data Intelligence

Human threat actors pose a major problem for the security of organizations' web applications. According to the Association of Certified Fraud Examiners (ACFE), businesses lose an estimated 5% of their annual revenues to fraud.[1] Cybercrime stands out as one of the most common forms of fraud, partly due to the increase in mobile and online transactions and the risks they introduce.

Cyber Risk is Business Risk

In 2022, losses due to cyberattacks and cyber-enabled fraud surged by 48% to $10.2 billion, up from $6.9 billion in 2021, as reported by the Federal Bureau of Investigation.[2] Grant Thornton projects online fraud and scams could potentially cost firms $10.5 trillion by 2025,[3] driven by the increased sophistication of attackers and their techniques. While security measures such as strong passwords, continual software updates, firewalls, bot defense systems, dedicated fraud detection platforms, and other security controls can indeed serve as deterrents against certain types of fraud, modern-day fraudsters are all too often successful at bypassing these defenses.

Unmasking Fraud

Optimal fraud detection is best achieved when tackled as a team effort with strong collaboration between security and fraud teams, coupled with the effective use of data and analytics that monitor activities across the entire user journey—from account creation to transaction processing. By collecting and assessing behavioral, network, and device data in-real time, organizations can increase their ability to detect and mitigate risks including account takeover (ATO), fraudulent account opening fraud (AO), and other types of security risks and cyber fraud.

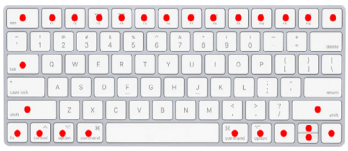
KEY FEATURES

Real-time actionable and contextualized telemetry signals (end user behavior, network, and device intelligence) that optimize fraud operations

Augment existing fraud ecosystems with rich telemetry signals to reduce risk and fraud losses. Gain a multi-dimensional view of digital identity risk.

Example:

.06% 49%



Keyboard usage pattern:
Fraudsters tend to rely on keyboard shortcuts and switch in and out of the browser.

Layered fraud protection

Enhance your ability to detect fraud with high-fidelity data intelligence collected from each user session to differentiate legitimate users from malicious human actors. Unique insights into identity events and consumer application activity provide a new dimension to traditional fraud detection tools

Digital identity DNA

Responsible for protecting the assets for over 40% of the Fortune 500 B2C enterprises, F5 has mastered the art of data collection and has amassed a large collection of proprietary, actionable information. A lead contributor to JavaScript enhancements, F5 understands the DNA of browsers and mobile devices and is unique in its ability to capture a wide range of behavioral telemetry.

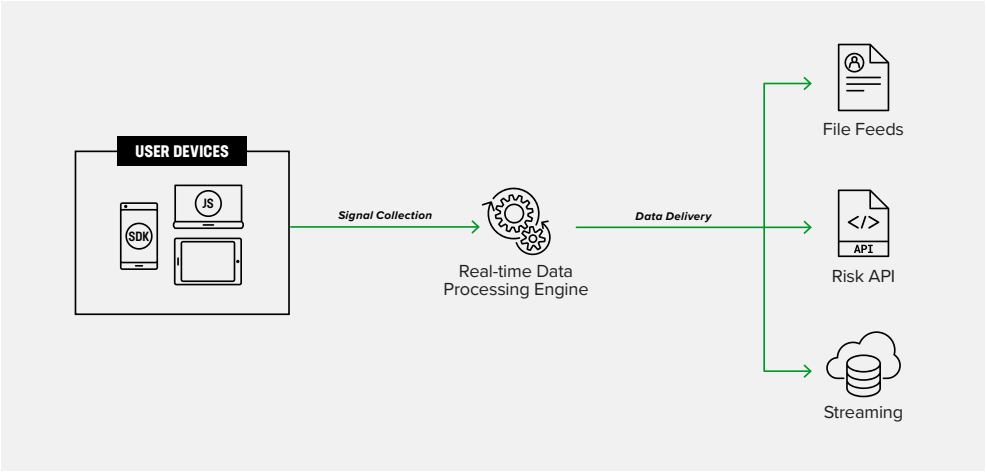


Figure 1. How it works

Empower Security and Fraud Teams to Detect Risky Behaviors That Suggest Malicious Intent

F5® Distributed Cloud Data Intelligence provides security, fraud, and network teams high-fidelity, refined intelligence about user behavior, network, and device characteristics to aid in unmasking fraud. Fraud detection and mitigation is best achieved when organizations have a holistic, multi-dimensional view of the entire user journey and have access to digital identity data that matters.

The ability to detect security and fraud risks can be significantly increased by blending behavioral biometrics (mouse movements, keyboard usage patterns, and unusual application interactions), device data (device identifiers, browser anomalies, and login patterns), and network characteristics (IP address and reputation, VPN, etc.), with the existing context and signals you already possess. By augmenting existing security, fraud, and authentication systems with Distributed Cloud Data Intelligence, organizations can create better rules and models to produce better quality data, resulting in fewer false positives, fewer false negatives, and overall greater fraud detection. Bringing context to the complex can mean the difference between thwarting a fraud attack and recovering from one.

Rich JavaScript obfuscation
F5's JavaScript obfuscation technology defends against reverse engineering by even the most sophisticated fraudsters—ensuring high accuracy of behavioral signal data collection

Seamless integration and ease of data ingestion
Distributed Cloud Data Intelligence is easily enabled by deploying a lightweight JavaScript bundle across all web pages. Choose how to receive data (API methods, file transfers, or streaming into a cloud service).

ADD CONTEXTUALIZED BEHAVIORAL BIOMETRICS, DEVICE DATA, AND NETWORK INTELLIGENCE TO EXISTING FRAUD MODELS TO DETECT AND MITIGATE FRAUD BEFORE HARM IS DONE.

Conclusion

Human threat actors pose a major problem for organizations' web application security. Gaining access to high-fidelity refined intelligence around user behavior, network characteristics, and device identification can help you more effectively detect malicious human actors—and prevent account takeover and fraudulent account opening.

Leverage F5 Distributed Cloud Data Intelligence to detect risky behaviors that suggest malicious intent. Detect and mitigate fraud early in the user lifecycle before harm is done by having access to the right data at the right time—without being overwhelmed by noise and unactionable data.

Next Steps

- Read the DevCentral article that introduces F5 Distributed Cloud fraud and risk solutions in a multi-method approach.
- Watch the on-demand webinar—Unmask Fraud: Account Takeover Detection with F5 Distributed Cloud Data Intelligence to discover how to unmask malicious human threat actors by leveraging rich user- and device-based.
- Get started today. Contact an expert at sales@f5.com to arrange a demo. For more information, visit our Distributed Cloud Services page at f5.com/cloud.

[1] Annette Greene, Fraud: Trends to look for, found at https://www.dla.mil/About-DLA/News/News-Article-View/Article/3106718

[2] Federal Bureau of Investigation Internet Crime Report, found at https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

[3] Three threats the mid-market saw coming for 2023, found at https://www.grantthornton.global/en/insights/international-business/three-threats-the-mid-market-saw-coming-for-2023