Distributed Cloud Data Intelligence

KEY BENEFITS

Richer Insights
Delivers high fidelity refined intelligence to ingest into an existing decisioning engine and enhance detection.

Reliable Device Identification
Provides a holistic view of trusted devices using real-time data and delivers intelligence that is useful for detecting fraud.

Behavioral Biometrics
Provides risk insights based on how users interact with the application and analyzes digital behaviors to help identify potential fraud.

Bridging Security and Fraud Teams
Data intelligence delivers actionable insights derived through visibility throughout the enterprise to help bridge the gap between security and fraud teams.

What is Data Intelligence?

Distributed Cloud Data Intelligence provides application defenders (i.e., network, security, and fraud teams) high fidelity refined intelligence around user behavior, network characteristics, and device characteristics that are useful for detecting malicious traffic.

Data Intelligence Delivers:

- Behavioral biometrics such as mouse movements, keyboard usage patterns, unusual interaction
- Network characteristics related to the original network infrastructure
- Device features such as device identifiers, browser anomalies, login patterns

Application defenders can seamlessly integrate with their existing decision engines to look at security, fraud, and authentication challenges in a holistic way. Using data from Data Intelligence in addition to context/signals that customers already have access to from other data sources, customers can build better rules and models and make decisions that result in fewer false positives and fewer false negatives.

What differentiates Data Intelligence?

Superior Data Collection

Safeguarding ~40% of B2C enterprises in the F500 from intense bot attacks, F5 developed profound depth in data collection, and at this point has a large collection of proprietary actionable data. F5's domain experts, including members of JavaScript specification committee TC-39, continuously research changes to JavaScript engines and browser APIs to identify subtle and effective data intelligence which strongly differentiate between legitimate and illegitimate users. Customers of Data Intelligence benefit from the continuous R&D that F5 invests in defending the world's most valuable websites.

SEAMLESSLY INTEGRATE WITH THE EXISTING FRAUD (AND SECURITY) ECOSYSTEM, EXISTING PROCESSES AND PROCEDURES, EXISTING STAFF SKILL SETS, AND TO EMPOWER ALL OF THOSE WITH HIGH FIDELITY, ACTIONABLE INTELLIGENCE AROUND BEHAVIORAL BIOMETRICS, NETWORK CHARACTERISTICS, AND DEVICE CHARACTERISTICS.

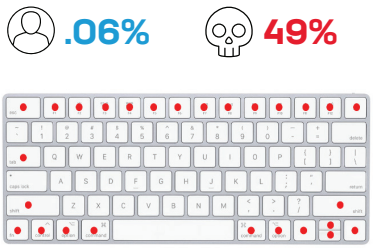
Obfuscated Client Code

Proprietary features are only useful if they can be secured against reverse engineering by the most sophisticated fraudsters in the world. In the decades F5 has spent in battling automated attacks in real-time, F5 has developed the most powerful JavaScript (JS) obfuscation technology in the industry, which safeguards our signal collection.

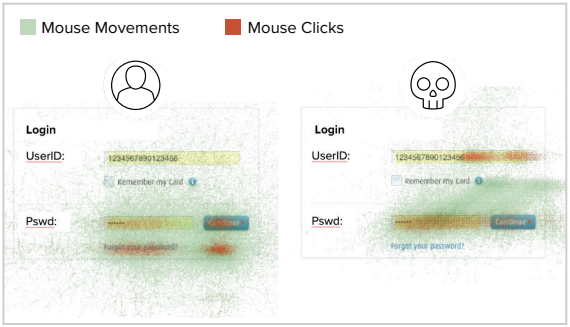
Ease of Use

Data Intelligence (for browsers) is enabled by deploying a lightweight JS bundle across all the web pages. This can be done via many different deployment methods, including F5 infrastructure. Customer fraud teams can choose API methods, file transfers or streaming into cloud services to build their own solutions using features from Data Intelligence.

Example:

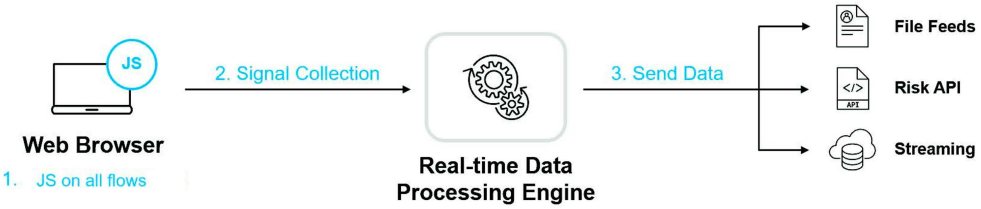


Keyboard usage pattern:
Fraudsters tend to rely on keyboard shortcuts and switch in and out of the browser.



Mouse Movements
Humans are often clumsy and inefficient, while fraudsters know their way.

How does Data Intelligence work?



F5 takes data privacy seriously and is compliant with privacy regulations.

Distributed Cloud Data Intelligence is a cloud-based curated data service dedicated to providing high fidelity data for protecting your applications. A JavaScript tag collects client signals and securely communicates with a real-time data processing engine to create and deliver the data to the customers.