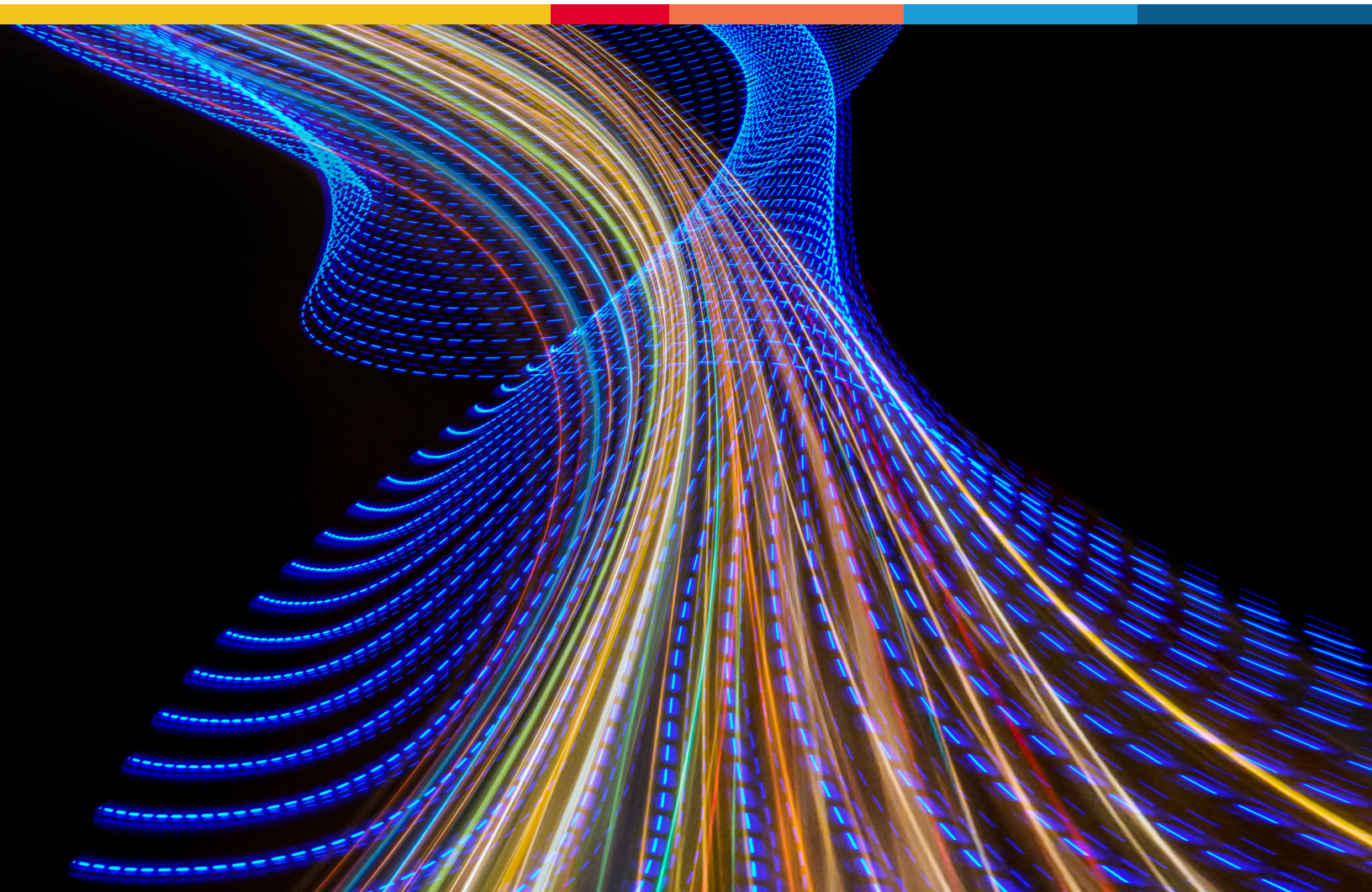
SOLUTION OVERVIEW

Gain the Benefit of Data Aggregators without the Risk

F5 Distributed Cloud Aggregator Management enables financial institutions to mitigate the potential security and fraud risks posed by aggregators, while harnessing the power of open banking to innovate and drive revenue growth.



KEY BENEFITS

Gain visibility and control
Identify aggregator traffic and establish volume and data access limits on a per-aggregator basis.

Mitigate security and fraud risk
Block attacks from malicious actors posing as legitimate aggregators–prevent credential stuffing that can lead to account takeover (ATO) and fraud.

Ensure optimal application performance and digital experiences
Prevent high volumes of aggregator traffic from overloading infrastructure and impacting service.

Generate new revenue opportunities
Leverage aggregators to create new, enhanced, and innovative product and services to drive customer expansion and uptake.

Financial Data Aggregators Drive Innovation, Introduce Potential Risks

Aggregators and third-party-providers (TPPs) enrich consumers' financial digital experiences and are increasingly becoming valued business partners for financial institutions. While digital channel teams at financial institutions look to leverage the strategic gains that collaborating with authorized aggregators can provide, security teams struggle to ensure aggregators do not misuse or expose customer data.

To combat the security risks posed by aggregators, financial institutions must gain visibility and access controls over aggregator and API traffic. They must be able to automatically detect when aggregator channels are being used by attackers to launch credential stuffing attacks or commit fraud. Without establishing fine-grained controls over aggregators, financial institutions leave themselves and their customers exposed to security and fraud risks.

Screen scraping by unauthorized aggregators poses one of the biggest threats for financial institutions. It occurs when consumers willingly share their username and password with aggregators who then use scraping technology to log into the customer's account to access information. This technique leaves banks in the dark since aggregators can access accounts without a relationship with the financial institution. This is a concern for financial institutions since they cannot enforce data access compliance checks on aggregators, yet they are responsible for breaches that occur from scraped data. This is one of the key reasons why the EU and the UK PSD2 included the requirement for financial institutions to provide approved third-party-providers and aggregators access via secure and standardized APIs.

In the US, where 90% of consumers rely upon some form of aggregator services, some larger banks have sanctioned API channels specifically for aggregators to help better protect data. However, screen scraping remains the common method for aggregators to access account data. As the open banking industry morphs and evolves, financial institutions must continue balancing consumer demands for enhanced digital experiences while protecting the interests and assets of all parties involved. Distributed Cloud Aggregator Management is the answer.

Manage Data Aggregator Security Risks While Enhancing Customer Value

F5® Distributed Cloud Aggregator Management enables financial institutions to ensure aggregators and third-party providers cause no harm. By providing mechanisms to manage aggregator activities to protect applications, APIs, and consumer data, Distributed Cloud Aggregator Management enables consumers to gain the enhanced digital experiences provided by aggregators and allows financial institutions to fully leverage the gains aggregators can provide—all while preventing customer data from being compromised.

KEY FEATURES

Authentication visibility
Labels traffic as human, automated, or aggregator.

Least privilege access
Enforces adherence to access policies mapped to approved characteristics (such as IP addresses, shared header values, and so on).

Rogue aggregator detection
Identifies and mitigates rogue aggregators attempting to access data.

Anomaly detection
Alerts on unusual traffic volume increases and drops in login success rates for approved aggregators—often signs of credential stuffing or account takeover attempts.

Violation alerting
Alerts when approved aggregator exceeds predefined time/volume limits.

Distributed Cloud Aggregator Management is a managed service that combines intelligence from a global network of known aggregators from the world's top financial services firms and the power of our rules assisted machine learning engine, powerful AI, and team of data scientists, to continually monitor aggregator traffic and take corrective actions to ensure aggregators adhere to agreed upon usage policies.

Understand Aggregator Traffic

Provides real-time visibility and analysis of aggregator transactions, making it possible to identify the aggregators accessing data, assess the traffic volume each aggregator produces, examine the data they access, and determine the channels being used.

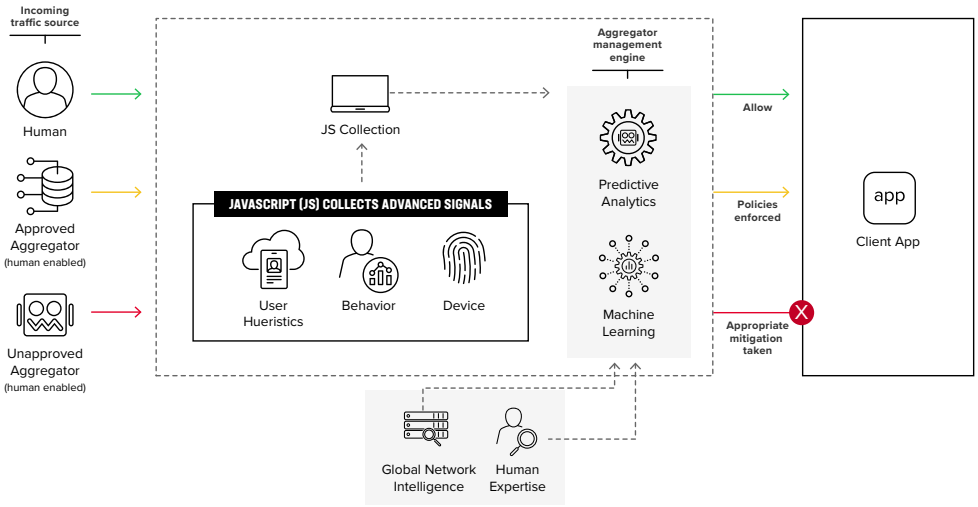


Figure 1: Increase visibility, enforce policy access rules, prevent attacks.

Manage Aggregator Actions

Enables financial institutions to set policies and controls that ensure approved aggregators only access allowed data using authorized channels within pre-approved limits. Aggregators that have relationships with the bank are allowlisted and their channels are monitored for anomalous activities from attackers. Aggregators that do not have a relationship with the bank are blocked when attempting to screen scrape customer data. By monitoring activities, malicious actors attempting to use aggregators as attack vectors are detected and mitigated.

AGGREGATORS CREATE A MYRIAD OF NEW OPPORTUNITIES FOR FRAUDSTERS. PROTECTING AGAINST SECURITY AND FRAUD RISKS INTRODUCED BY ROGUE AGGREGATORS IS NOT EASY.

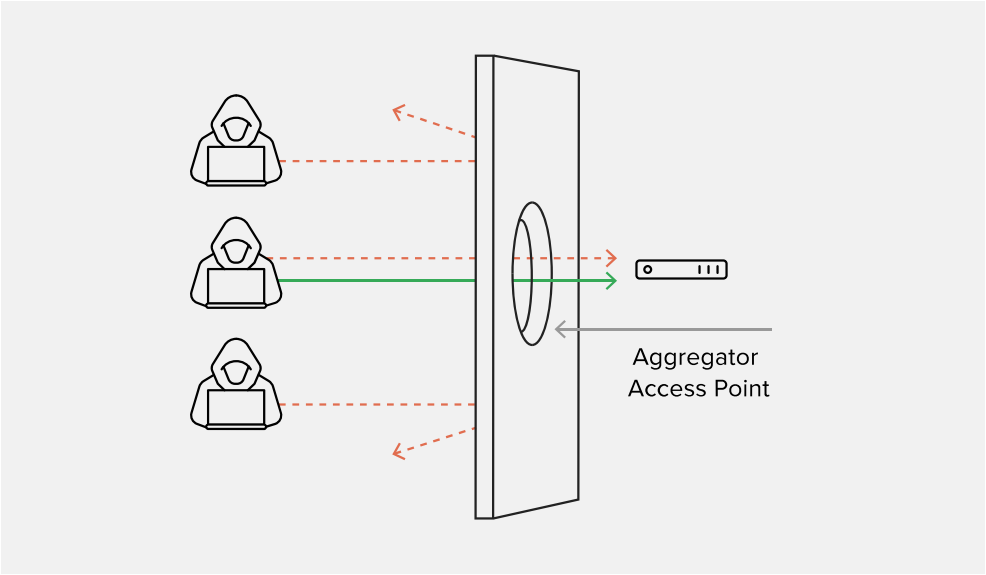


Figure 2: Bad actors look to exploit aggregators as attack vectors.

Optimize Application Uptime and Reduce Infrastructure Costs

Prevents large volumes of aggregator traffic from overwhelming existing infrastructure. This is critical given aggregator volume may comprise between 50-60% of overall traffic.

Mitigate Compliance Breaches

Enables financial institutions to establish and enforce policies to ensure aggregators only access approved data using authorized channels and under pre-defined limits—reducing the risk of compliance breaches.

Minimize Customer Friction, Enhance Customer Experiences

Ensures consumers' digital experiences are not compromised by preventing system latency and account takeovers.

Conclusion

Open banking is driving innovation, providing consumers with enhanced digital banking experiences and data aggregators are playing a key role—presenting both opportunities and challenges for financial institutions and their customers.

Financial institutions, once hesitant to share client data with financial aggregators due to privacy concerns, have come to realize data aggregators can provide value for them and convenience for their customers. But without establishing fine-grained controls over aggregators, financial institutions expose themselves and their customers to security and fraud risks.

F5 Distributed Cloud Aggregator Management provides the controls financial institutions need to securely embrace data aggregators and leverage their innovations to create new and enhanced product and service offerings—driving new revenue opportunities and boosting customer uptake and retention.

Find out how F5 Distributed Cloud Aggregator Management can help you embrace data aggregators to innovate without compromise. Get started today. Contact an expert at sales@f5.com to request a demo.

©2022 F5, Inc. All rights reserved. F5, and the F5 logo are trademarks of F5, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com.
Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, expressed or implied, claimed by F5, Inc.
DC0422 | OV-XC-843297800