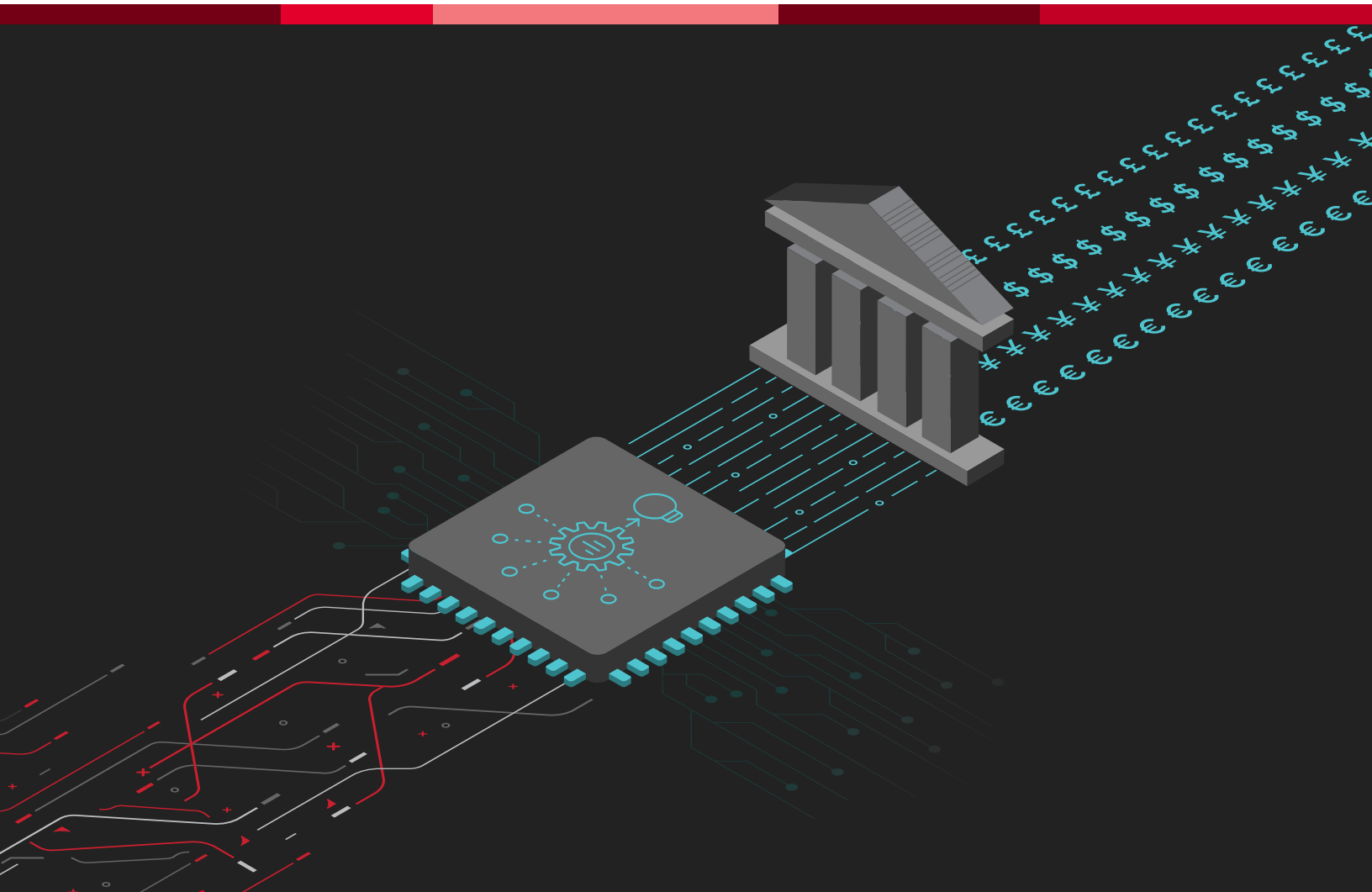
CASE STUDY

F5 Helps a Digital Bank Detect 177% More Fraud Than Existing Fraud Solutions



HOW A FINANCIAL COMPANY IS BENEFITING FROM F5 DISTRIBUTED CLOUD ACCOUNT PROTECTION

Reliably detecting and eliminating fraud is driving:

1. Detection of significant additional fraud
2. Low false positive rates (FPR)
3. Better fraud operations performance
4. Decreased fraud losses and increased profit

COVID-19 has accelerated the digital shift by at least two years. As per BAI, an independent non-profit organization, digital banking is moving out of the "early majority" curve and into the "late majority" phase of technology adoption. In its research BAI found that over half of banking customers use digital products more since the pandemic, and that 87% of them are planning to continue this increased usage after the pandemic. This creates an increased digital attack surface for fraud.

The pandemic has also resulted in increased efforts to steal customer information via methods like smishing/phishing, social engineering scams, and other methods. Combatting this activity requires a holistic fraud solution that simultaneously reduces fraud and improves the online customer experience.

Per the Experian Global Identity and Fraud Report:

- Mobile Account Takeover (ATO) has doubled over the last four years
- Retirement account fraud has increased 180% in the last year

The Customer: A North American Bank

A North American digital bank with over $1B in AUM and millions of customers was looking to cut fraud losses. Over 90% of the bank's customers transact online. The main interaction for retail banking customers occurs via web and mobile applications.

The Problem: Account Takeover Fraud and Account Opening Fraud

The bank has seen peak fraud losses due to COVID-19, and losses in May 2020 alone were some of the largest they had ever seen. Fraudsters took over victim accounts (ATO–Account Takeover fraud) and conducted several fraudulent money transfers via online banking. The fraudsters also created several fraudulent accounts (AO–Account Opening fraud), using stolen identities (third party fraud) and synthetic identities (first party fraud). Fraudsters used these accounts as drop accounts to exploit several COVID-19 government benefits packages, wherein they conducted ATO fraud at other banks and credit unions and transferred money into this bank's drop accounts. Also, several of the bank's customers fell victim to targeted smishing/phishing campaigns. The bank found that 60% of fraud came from ATO and 40% from AO. Over 60% of the fraudulent activity came in the form of non-monetary activity (address change, adding a payee, etc.) This was activity fraudsters did to test the waters

before they transferred money. The bank had a leading device identifier solution and a legacy fraud engine in place. These systems were unable to detect over 80% of the fraud discussed above.

WHY F5?

F5 is a trusted leader in providing application security. The same AI-powered precision F5 offers to accurately detect attack traffic in real-time to secure applications can now be offered to reliably detect and eliminate online fraud.

The Solution: Bottomline Fraud Loss Reduction

Reliably detecting and eliminating additional fraud. F5 proposed to this bank that it could reliably detect and eliminate significant additional fraud without adversely affecting business operations. F5 offers a solution called F5® Distributed Cloud Account Protection that leverages the power of artificial intelligence and F5's network insights to safely and accurately identify fraudulent transactions, so that companies can eliminate the losses due to these fraudulent transactions. With Distributed Cloud Account Protection, F5 offered this bank the ability to identify additional fraud without impacting its business operations. This resulted in a significant decrease in losses.

Below are the typical steps in an account takeover (ATO):

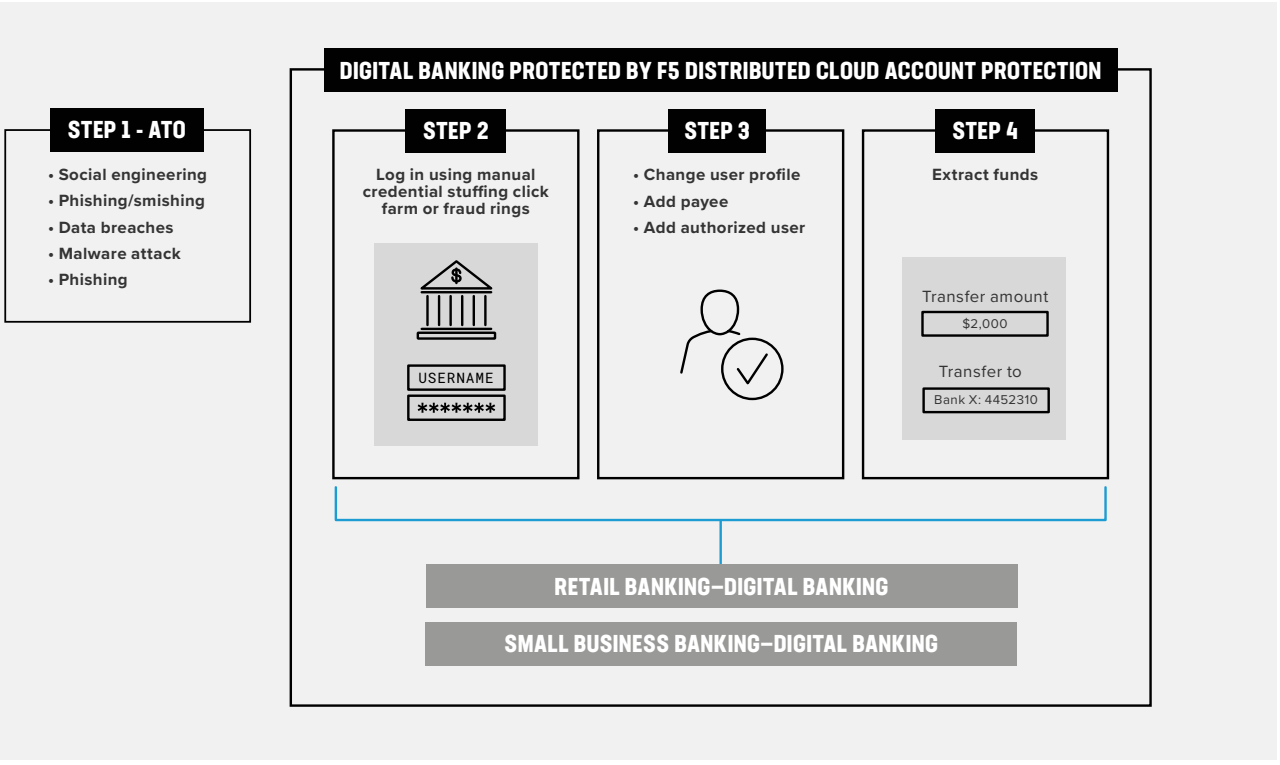


Figure 1: Typical ATO steps

The Results

Distributed Cloud Account Protection immediately showed significant value for the customer with a low False Positive Rate (FPR):

- At a 0.1% FPR, the service detected an additional 177% in fraud, saving $6.2M annually
- At a 0.5% FPR, the service detected an additional 276% in fraud, saving $9.7M annually

The data pointed to the following conclusions:

Distributed Cloud Account Protection reliably detects and eliminates significant additional fraud. For this bank, the service detected and eliminated a significant amount of additional fraud with an extremely low false positive rate when compared with its current solution.

Distributed Cloud Account Protection leads to decreased fraud losses. The bank's annual fraud losses, primarily from Account Takeover (ATO) and Fraudulent Applications (FRAP), have been significantly reduced since the service was deployed.

Distributed Cloud Account Protection does not adversely impact business operations. The service yielded marked, tangible results without negatively impacting the business environment.

Reliably Detecting Fraud without Adversely Impacting Business Operations

Distributed Cloud Account Protection gives fraud teams a new and powerful solution to detect and eliminate online fraud.

The unique telemetry of Distributed Cloud Account Protection is focused on understanding intent. The service can connect context across different browsers and devices used by the same user, as well as observations from across F5's entire network.

Distributed Cloud Account Protection feeds this data and enterprise fraud files into an AI engine that determines a single, high-fidelity, real-time outcome.

The solution delivers significant reductions in fraud immediately and continues to drive down fraud each and every month as the AI engine consumes more data and continues to learn.

To learn more, contact your F5 representative, or visit f5.com.