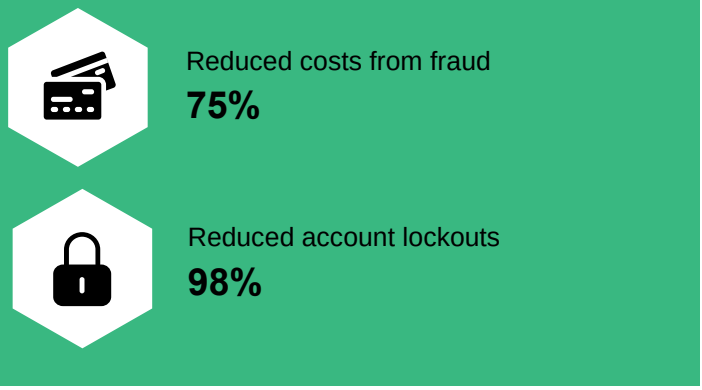
FORRESTER®

Financial Services Firms Reduce The Costs Of Bot Attacks And Improve Customer Experience With F5®

Financial services firms face constant account takeover attacks from automated bots that leverage stolen credentials with the aim of committing fraud. The need to defend against such attacks leads to high operating costs for both security teams and fraud departments while negatively impacting customers' experience via account lockouts, password resets, and support requests.

F5 brings automated bot defense to financial services firms, reducing the number of successful bot attacks and saving time for security teams and fraud departments. Financial services organizations leveraged the F5 anti-bot and antifraud solution to reduce their costs of fraud, mitigate credential-stuffing attacks, limit account lockouts, and lower their ongoing security costs, all while improving their overall customer experience.

To better understand the benefits and costs associated with the F5 Distributed Cloud Bot Defense solution, F5 commissioned Forrester Consulting to interview five decision-makers and conduct a Total Economic Impact™ (TEI) study.[1] This abstract will focus on the financial services industry's use of F5 and its value to their organizations.



INVESTMENT DRIVERS

The interviewees' organizations faced a number of security challenges. These included:

- **High customer friction.** Regardless of prior protections put in place, financial services firm interviewees experienced a high number of bot attacks each year. These attacks resulted in high customer friction from successfully stolen login credentials, account lockouts, the need to reset passwords, and calls to customer support.
- **High burden of fraud investigations.** Without sufficient bot protection, financial services interviewees' antifraud work fell to downstream fraud investigation processes. F5 Distributed Cloud Bot Defense allowed these firms to automate blocking of fraudulent activity in real time, leaving fraud professionals more time and energy to focus on human fraud.
- **High cost of manual bot protection.** Financial services firms without existing third-party bot protection relied on manual workstreams to counteract bot-induced fraud. Using a conventional web applications firewall (WAF) and other firewalls, security teams investigated traffic and blocked IP addresses manually and constantly. This was not only less effective, but it also incurred high labor costs, distracted security professionals from more important work, and reduced their satisfaction with their jobs.

READ THE FULL STUDY HERE

> **"Our security teams saw lots of incidents and had to deal with a lot of tickets before [Distributed Cloud Bot Defense]. It was pretty much whack-a-mole and writing rules day-to-day, every day. Now we can just update our rules once, maybe twice a month max."**
>
> *Senior manager of network protection, financial services*

F5 DISTRIBUTED CLOUD BOT DEFENSE FEATURES

F5 enabled financial services firms to solve the previous challenges by leveraging several features, including:

- **Automated bot defense.** Cybercriminals leverage a rapidly changing landscape and automated attack frameworks to take over customer accounts utilizing bots and ultimately execute fraudulent transactions and obtain lines of credit. F5 Distributed Cloud Bot Defense mitigates bots and malicious automation, prevents tampering, and shifts mitigation strategies to ultimately deter compromise.
- **Real-time protection and visibility.** Cybercriminals will also quickly change tactics to find weaknesses, including attacking financial institutions through third-party APIs and aggregators. F5 Distributed Cloud Bot Defense deters fraud and abuse with omnichannel protection, real-time and historical intelligence, and continuous oversight to ensure financial services firms can innovate without increasing risk.
- **High security effectiveness.** False positives result in missed business opportunities and increase customer friction. Through telemetry collection, multistage detection, artificial intelligence, and continuous monitoring, F5 Distributed Cloud Bot Defense provides high security while minimizing false positives, reducing the risk of transaction and revenue abandonment.

> **"It's very, very important to us that we not introduce customer friction. Because of this, CAPTCHA was not an option from day one."**
>
> *Executive director, financial services*

KEY RESULTS

Leveraging these features delivered a number of benefits to financial services firms' digital security environments and operations. These benefits include:

Financial services firms use F5 to reduce the cost of fraud by as much as 75%. Before investing in the F5 Distributed Cloud Bot Defense solution, interviewees from financial services shared experiencing a high amount of bot activity that resulted in fraudulent account-related activities, such as account creation, credential stuffing, and account takeovers. F5 Distributed Cloud Bot Defense enabled these firms to decrease bot attacks and substantially reduce the costs of bot-related fraud as a result. Financial services interviewees noted improving their blocking rate by up to 90% and reducing their fraud by as much as 75%.

- "F5 saved us a lot of money related to the automated bot attacks resulting in successful fraud." – *Executive director, financial services*
- "With F5, my security team can stop the high-volume automated fraud tactics so the fraud team can tune their models to catch the anomalous

human behavior." – *Executive director, financial services*

F5 enables financial services organizations to reduce costs from credential-stuffing attack costs by 96%. Before F5's Distributed Cloud Bot Defense, interviewees from financial services firms said their organizations experienced upwards of 50 credential-stuffing attacks annually at an estimated per-attack cost of $500,000. Included in such costs were the dozen or so employees who spent multiple hours weekly investigating and mitigating these attacks. With F5, the number of such attacks falls to around two annually, or by about 96%.

- "We were seeing multiple P1 incidents from credential-stuffing attacks before implementing F5's Distributed Cloud Bot Defense, and now we're only dealing with one every six months or so." – *Executive director, financial services*
- "Successful credential stuffing is basically gone now thanks to F5." – *Executive director, financial services*

Financial services firms also reduce account lockouts by as much as 98%, saving on customer support expenses and improving user experience. Before F5, financial services firms' customer experience suffered. Bot attacks led to customers being locked out of their accounts, having to reset their passwords, needing customer support to unlock accounts, and experiencing latency and downtime of applications. With F5 Distributed Cloud Bot Defense, financial services interviewees report password reset requests falling by up to 80% and account lockouts shrinking by as much as 98%.

- "Not only has F5 saved us money on fraud, but it also saved our customers time in having to reset their passwords multiple times." – *Senior manager of network protection, financial services*
- "We went from 19,000 to 20,000 customers being locked out of their accounts daily to just hundreds." – *Executive director, financial services*
- "Reducing customer password resets and account lockouts also reduced the number of calls in to support and those costs." – *Senior manager of network protection, financial services*

> **"I would need double my current team size to do the work [F5] is doing for us."**
>
> *Senior manager of network protection, financial services*

Automation from F5 enables financial services firms to improve the efficiency of their security teams by as much as 100%. Before F5 Distributed Cloud Bot Defense, bot attacks forced financial services firms' security teams to spend a lot of their time on investigations, rule updates, and manual processes to defend against such attacks. Not only did F5's solution reduce the security team's tasks related to all of these processes, reducing costs, it enabled these teams to focus on more pressing work and even bolstered the credibility of security teams internally.

- "Our investigation teams are at least 100% more productive. What used to take them a week can now be done in a couple days." – *Executive director, financial services*
- "Our security team is now able to focus on internal reviews, finding other gaps, and patching holes in the vents so to speak." – *Senior manager of network protection, financial services*
- "Our security team definitely gets a lot more trust now. When we recommend a solution for something, our opinion matters now more than before." – *Senior manager of network protection, financial services*

TOTAL ECONOMIC IMPACT ANALYSIS

For more information, download the full study: "The Total Economic Impact™ Of F5® Distributed Cloud Bot Defense," a commissioned study conducted by Forrester Consulting on behalf of F5, February 2022.

STUDY FINDINGS

Forrester interviewed five decision-makers at organizations with experience using F5 and combined the results into a three-year composite organization financial analysis. Risk-adjusted present value (PV) quantified benefits include:

- Reduced costs of fraud from bot attacks by 30%.
- Reduced costs from credential-stuffing attacks by 96%.
- Reduced account lockouts and their cost to support by 88%.

Return on investment (ROI)

195%

Net present value (NPV)

$6.42M

Appendix A: Endnotes

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.


FORRESTER®