



# Protect Apps and the Business

Organizations today find themselves at a critical inflection point: adapt or fail. 98% of organizations depend on applications to run or support their business,<sup>1</sup> and 80% are executing digital transformation initiatives to accelerate time to market.<sup>2</sup>



## KEY BENEFITS

### Unparalleled Visibility

F5 powers more than half of the world's applications across all types of environments, protects over 1 billion transactions daily from application attacks on the largest companies, and ensures more than 200 million legitimate human transactions are kept safe every day.

### Highest Real-World Security Efficacy

F5 can uniquely provide long-term, persistent efficacy, because its artificial intelligence algorithms are trained on attack profiles and risk surfaces of similar organizations.

### Improved Customer Experience

F5 solutions adapt and maintain full efficacy, even as attackers retool and evolve to overcome countermeasures. F5 solutions also reduce or remove high-friction mechanisms, including CAPTCHA and multifactor authentication, thereby improving the overall user experience.

SKILLED ATTACKERS ARE  
MOTIVATED BY PROFIT.  
THEY CONTINUALLY ASSESS  
WHICH TARGETS WILL  
PROVIDE THE HIGHEST  
RETURN ON THEIR  
INVESTMENTS.

**Innovative apps are essential for organizations that want to** be first to market, first to profit, and first to cool. Automation is a key strategy to help organizations facilitate this application revolution across technology, processes, and people. Unfortunately, attackers also have embraced automation to attack and abuse applications. Readily available tools, infrastructure, and compromised data result in low attack investment with high returns, creating attractive attacker economics.

Skilled attackers are motivated by profit. They continually assess which targets will provide the highest return on their investments.

Attacks are easy to implement, and their potential value is astronomical. As digital transformation and the use of applications for commerce continue to skyrocket, attackers will increasingly embrace automation and artificial intelligence (AI) to adapt to and overcome security countermeasures.

Commonly used mitigations such as CAPTCHA and Multi-Factor Authentication (MFA) are designed to validate human behavior and identity, but they often frustrate users while failing to provide the security they're meant to deliver. In reality, motivated attackers can bypass these defenses, which can create a wide range of costly problems for organizations that rely on them.

One in three customers will leave a brand they love after just one bad experience.<sup>3</sup>

## Adapting to Attacker Economics

Automated attacks continue to evolve, enabling bad actors to adapt and bypass basic security defenses with very little investment. These attackers typically leverage readily available infrastructure, such as bots and hacker toolkits, literally for pennies on the dollar.

The proliferation of architectures, cloud, and open-source software has expanded the risk surface for attackers. Application vulnerabilities such as injection and cross-site scripting continue to exist, even after 20 years of security best practices. It is no surprise that attackers leverage bots and automation to scan for these vulnerabilities and exploit them—with potentially disastrous outcomes, including data compromise.

BOTS ARE INCREASINGLY  
USED FOR COMMERCIAL AND  
RETAIL FRAUD.<sup>4</sup>

A successful attack can result in several business problems with serious impacts:

| Problem                           | Impact                     |
|-----------------------------------|----------------------------|
| Insight and visibility disruption | Poor business intelligence |
| Performance degradation           | Poor user experience       |
| Unauthorized access               | Data compromise            |
| Account takeover                  | Fraud                      |

Attacks vary in sophistication and often adapt to security countermeasures. For example:

- Automation that leverages bots to scan for application vulnerabilities
- Credential stuffing attacks that use readily available compromised credentials and tools
- Imitation attacks that employ tools to emulate human behavior to bypass defenses
- Manual attacks that leverage human click-farms or manual hacking to bypass defenses

Attackers invest along four vectors—often simultaneously—until they get past whatever defenses you may have:

- Emulating valid network traffic
- Emulating a variety of valid devices and browsers
- Emulating actual human behavior
- Using stolen credentials and personally identifiable information

ONE IN THREE CUSTOMERS WILL LEAVE A BRAND THEY LOVE AFTER JUST ONE BAD EXPERIENCE.<sup>3</sup>

An attack may use a variety of tools to adapt to and bypass mitigation countermeasures:

| Tool/Technique               | Use                                                                  | Mitigation                          | Adaptation                          |
|------------------------------|----------------------------------------------------------------------|-------------------------------------|-------------------------------------|
| SentryMBA                    | Construct tailored attacks                                           | IP Rate Limiting Text-Based CAPTCHA | Spoof CAPTCHA                       |
| CAPTCHA Solvers              | Bypass CAPTCHA challenges                                            | JavaScript injection                | Spoof JavaScript challenges         |
| Scriptable WebViews          | Full web stack emulation, including JavaScript                       | Header and environment checks       | Spoof header and environment checks |
| Scriptable consumer browsers | Full web browser emulation, including header and environment         | Browser fingerprinting              | Anti-fingerprinting                 |
| Anti-fingerprinting tools    | Randomize data sources used to fingerprint browsers                  | Behavioral analysis                 | Emulate human behavior              |
| Human behavior emulation     | Combine CAPTCHA solving, proxy rotation, and emulated human behavior | Browser consistency checks          | Use real browser data               |
| Use real data                | Cycle through real browser fingerprint data                          | User behavior profiling             | Human click-farms or manual hacking |

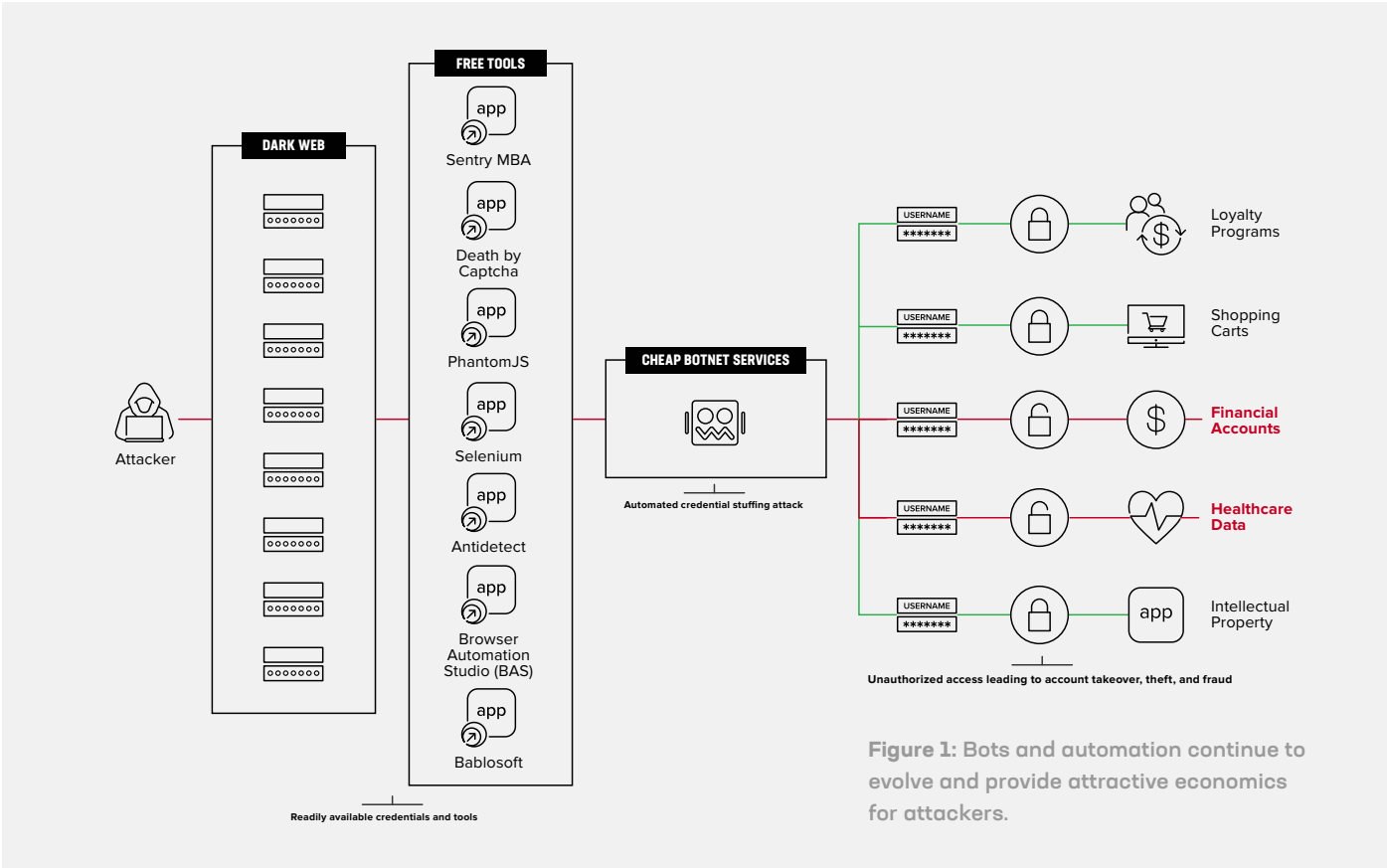


Figure 1: Bots and automation continue to evolve and provide attractive economics for attackers.

## KEY FEATURES

- Layered defenses protect bandwidth and services from performance degradation and outages
- Protection from credential stuffing mitigates unauthorized access and account takeover
- Client-side defenses prevent attacks that steal sensitive data through browser or third-party exploits
- Behavioral defenses slash fraud losses by protecting against imitation attacks that emulate human behavior
- Removal of high-friction mechanisms, including CAPTCHA and Multi-Factor Authentication (MFA), improves the overall user experience
- Threat intelligence across similar attack profiles and risk surfaces maximizes effectiveness
- Mitigations maintain full efficacy as attackers retool and evolve to overcome countermeasures—stopping the most advanced cybercriminals and state actors

# Neutralize Attackers by Mitigating Bots and Abuse

**Your customers demand simplicity. Your applications are complex. Your attackers are motivated.**

Security must adapt to attackers who retool to bypass countermeasures—regardless of the attackers' tools, techniques, or intent—without frustrating users with login prompts, CAPTCHA, and MFA. This includes omnichannel protection for web applications, mobile applications and API interfaces, protection against scans that attempt to exploit application vulnerabilities, and client-side defenses that prevent the theft of sensitive data through browser or third-party exploits.

Threat intelligence across similar attack profiles and risk surfaces provides unparalleled accuracy. This allows mitigations to maintain full efficacy as attackers retool and adapt to countermeasures—stopping even the most advanced cybercriminals and state actors.

This ability to react as applications and attackers adapt dramatically improves business outcomes, including:

- Reduced losses due to fraud and abuse
- Better application performance and uptime
- Measurable cost savings for hosting and bandwidth

## Conclusion

Security vendors must operate under the assumption that skilled attackers already have or soon will bypass all defenses. Attacker frameworks are predicted to leverage trained AI models to bypass security.<sup>5</sup>

The only viable defense is deterrence, disrupting attacker economics by making successful attacks too costly to be feasible.

F5 solutions adapt and maintain full efficacy, even as attackers retool and evolve to overcome countermeasures. F5 solutions also reduce or remove high-friction mechanisms, including CAPTCHA and multifactor authentication, thereby improving the overall user experience.

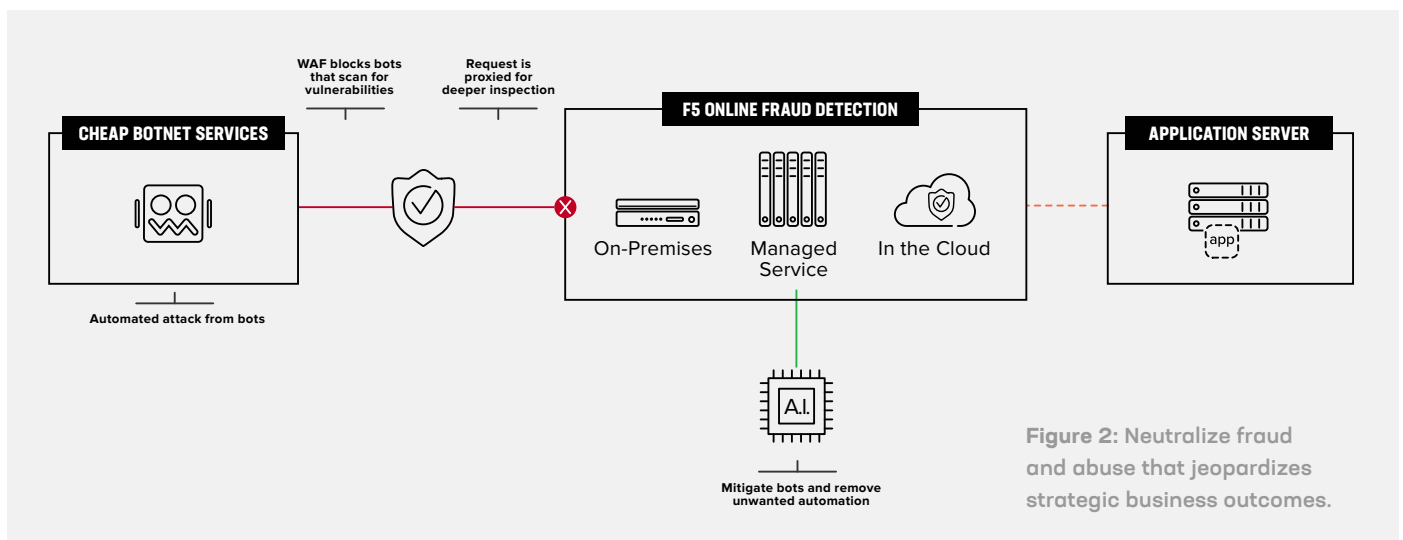


Figure 2: Neutralize fraud and abuse that jeopardizes strategic business outcomes.

To learn more, explore [F5 Application Security](#).

<sup>1</sup> 2020 State of Application Services Report, 8, found at <https://www.f5.com/state-of-application-services-report>

<sup>2</sup> Ibid, 7.

<sup>3</sup> 37 Customer Experience Statistics You Need to Know for 2020, found at <https://www.superoffice.com/blog/customer-experience-statistics/>

<sup>4</sup> International Botnet and IoT Security Guide 2020, found at [https://securingdigialeconomy.org/wp-content/uploads/2019/11/CSDE\\_Botnet-Report\\_2020\\_FINAL.pdf](https://securingdigialeconomy.org/wp-content/uploads/2019/11/CSDE_Botnet-Report_2020_FINAL.pdf)

<sup>5</sup> Shape Security Predictions 2020, found at [https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape\\_Security\\_Predictions\\_2020\\_Report\\_-\\_Emerging\\_Threats\\_to\\_Application\\_Security.pdf](https://info.shapesecurity.com/rs/935-ZAM-778/images/Shape_Security_Predictions_2020_Report_-_Emerging_Threats_to_Application_Security.pdf)

