Case Study of Leading Agricultural Banking Firm

PROJECT: F5 AWAF Implementation

CLIENT: LEADING AGRICULTURAL BANKING FIRM

LEADING AGRICULTURAL BANKING FIRM Background

Over four decades, it has transformed lives in Indian villages through agri-finance, infrastructure development, banking technology, microfinance, and rural entrepreneurship. LEADING AGRICULTURAL BANKING FIRMsupports nation building through participatory financial and non-financial interventions, innovations, technology, and institutional development in rural areas. It also provides capacity building in agriculture and rural development to officials of rural financial institutions, NGOs, and MFIs.

LEADING AGRICULTURAL BANKING FIRMis a Development Bank with a mandate for providing and regulating credit for the development of agriculture, small-scale industries, cottage and village industries, handicrafts and other allied economic activities in rural areas to promote prosperity of rural areas. It has 336 District Offices across the country which are staffed by District Development Managers (DDMs).

CHALLENGES

1. Automated attacks and bots overwhelm existing security solutions
2. Malware and keyloggers steal data and credentials to gain unauthorized access to user accounts
3. Application-layer attacks evade signatures and reputation-based security solutions

Need for Solution

The need for secure, scalable, high-performance, and reliable infrastructure being the need of an hour for customer and as web attacks are the leading cause of data breaches. Despite the best efforts of secure application- and patch-management processes, half of all applications remain vulnerable, 24x7. A solution which could scan for all such threats in the incoming traffic and can protect the web applications from vulnerabilities and web attacks while maintaining the requirement of mitigating such vulnerabilities and safeguarding their user data.

A solution known as BIG IP Advanced web application firewall (AWAF) that identifies and blocks attacks other WAFs miss. BIG-IP Advanced WAF delivers a dedicated, dynamic dashboard ensuring compliance against threats listed in the OWASP Top 10, guided

configurations for common WAF use cases, learning engine and customized policy building, and granular security policies for microservices and APIs that protects web applications from a variety of application layer attacks such as cross-site scripting (XSS), SQL injection, and cookie poisoning, among others was introduced.

Advanced Web application firewalls (AWAF) protect your applications from data breaches by fixing vulnerabilities and stopping attacks. F5® Advanced Web Application Firewall™ provides malicious bot protection, application-layer encryption, API inspection, and behaviour analytics to help defend against application attacks.

Identify and block attacks other WAFs miss

Protects your applications with behavioural analytics, layer 7 DoS mitigation, application-layer encryption of sensitive data, threat intelligence services, and API security.

- **Application-Layer Attacks** - Application-layer attacks can evade signature and reputation-based security solutions.
- **Web App and API Attacks** - New application attack surfaces and increased threat thresholds are popping up due to the rapid adoption of APIs (ex. GraphQL APIs, OWASP Top 10).
- **Security Automation for DevOps** - Bring apps to market faster with lower cost and higher security efficacy.
- **Targeted Attack Campaigns** - Active attack campaigns are difficult to detect from singular attacks.
- **Automated Attacks and Bots** - Automated attacks and bots can overwhelm application resources.
- **Credential Theft** - Attacks that steal application credentials or take advantage of compromised accounts.

F5 Advanced WAF Features

- **Proactive Bot Protection**

Proactively defend your applications against automated attacks by bot and other attack tools. This prevents layer 7 DoS attacks, web scraping, and brute-force attacks. Proactive bot defense helps identify and mitigate attacks before they cause damage to the site.

- **DataSafe**

Protect sensitive information from interception by encrypting data while it's still in the browser. DataSafe encrypts data at the application layer to protect against malware and keyloggers. This renders leaked credentials or data useless.

- **Behavioral DoS**

Behavioral DoS provides automatic protection against DDoS attacks by analyzing traffic behavior using machine learning and data analysis. By continuously monitoring server health and load, anomalies (performance slowdowns or traffic spikes) can be accurately detected and mitigated as needed.

- **Flexible Deployment**

Available as a purpose-built appliance, a cloud-ready virtual appliance, or part of the F5 SAAS based solution.

Core Capabilities

1. **Advanced application protection**

   Combines machine learning, threat intelligence, and deep application expertise

2. **API protocol security:**

   Combines machine learning, threat intelligence, and deep application expertise

3. **Security as code:**

   Declarative API-based deployment and configuration enables delivering security as "code"

4. **In-browser data encryption:**

   Encrypts data at the app layer to protect against data-extracting malware and man-in-the-browser attacks

5. **Behavioral DoS:**

   Behavioural analytics and machine learning provide highly accurate L7 DoS detection and mitigation

6. **Defenses for the OWASP Top 10:**

   Defends critical apps from today's biggest security concerns, including those listed in the OWASP Top 10

7. **Stolen credential protection:**

   Protects against brute-force attacks that use stolen credentials

8. **Proactive bot defense:**

   Protects apps from automated attacks by bots and other malicious tools