WEB APPLICATION AND API PROTECTION CAPABILITIES:

A Checklist for Financial Institutions

Application programming interfaces (APIs) have enormous potential and ability to support interconnections among all manner of devices, applications, and data, are the technology underpinning a growing range of internal and external bank strategies and activities. They hold the promise of increased openness for more competition to benefit customers. Yet, the rapid growth of APIs in financial services has expanded the attack surface and introduced new security risks.

Embedding a web application and API security solution while planning, implementing, or optimizing your information security strategy will provide your organization with the ability to understand your unique risks, target security gaps, and detect threats. To remain competitive, financial institutions need a web application and API protection (WAAP) solution that provides continuous visibility with comprehensive insights, and the full capability to identify and stop the most sophisticated attacks.

This checklists can be used to assess vendor capabilities or as a list of requirements needed to implement an effective WAAP solution.

01. PLATFORM REQUIREMENTS

02. ADAPTIVE WEB APPLICATION AND DDoS PROTECTION

03. API VISIBILITY, PROTECTION, AND CONTROL

04. FLEXIBLE MANAGEMENT

01 PLATFORM REQUIREMENTS

- Scalability to match traffic demands and provide continuous protection without loss of performance
- Architecture that can overcome the challenges of geographically dispersed applications
- Audit log capabilities to ensure proper usage
- Protection of on-premises, private, or public cloud (including multi-cloud or hybrid-cloud) site origins
- Network layer [L3/4] distributed denial- of-service (DDoS) mitigation with a zero- second service-level agreement
- Visibility into who is attacking, the frequency of attacks, and the severity of attacks with crowd-sourced attack intelligence across the platform
- Reverse proxy with web traffic via ports 80 and 443
- Network privacy protections with SSL/TLS encryption
- A proven leader in the solution category for at least 5 years by an unbiased third party
- Automatically discover and alert when and where Personally Identifiable Information (PII) is being passed to protect against data leaks

Financial institutions are responsible for protecting sensitive customer and financial data from rapidly evolving security threats. To respond, your web application security solution should be flexible, scalable, and easy to administer.

ADAPTIVE WEB APPLICATION AND DDoS PROTECTION 02

Web application security must go beyond traditional signature-based detection to more advanced forms of adaptive web application and DDoS protection for the most accurate and reliable security outcomes.

- Detection beyond signature-based attacks with anomaly and risk-based scoring
- Fully managed WAF rules to eliminate the need for continuous configuration and updates
- Client reputation scoring and intelligence for both individual and shared IP addresses
- Machine learning, data mining, and heuristics-driven detection capabilities to identify rapidly evolving threats
- Automatic web application firewall (WAF) rule updates with continuous real-time threat intelligence from security researchers
- Ability to test new or updated WAF rules against live traffic before deploying to production
- Protection (at a minimum) against SQL injection, XSS, file inclusion, command injection, SSRF, SSI, and XXE
- Fully customizable predefined rules to meet specific customer requirements
- Protection from application layer [L7] volumetric DoS attacks designed to overwhelm web servers with recursive application activity
- Custom rules to quickly protect against specific traffic patterns (virtual patching)
- Request rate limits to protect against automated or excessive bot traffic
- Protection from direct-to-origin targeted attacks
- IP/Geography controls via multiple network lists to block or allow traffic from specific IP, subnet, or geographic areas
- Protection from automated clients, such as vulnerability scanning and web attack tools

03

API VISIBILITY, PROTECTION, AND CONTROL

- Automatic discovery and profiling of unknown and/or changing APIs (including API endpoints, characteristics, and definitions)
- Automatic inspection of XML and JSON requests to detect API-based attacks
- Rate controls (throttling) for API endpoints based on API key
- API network lists (allowlists / blocklists) based on IP/Geography
- API lifecycle management with versioning
- Custom API inspection rules to meet specific user requirements
- Secure authentication and authorization via JSON Web Token (JWT) validation
- Ability to predefine acceptable XML and JSON object formats that restrict the size, type, and depth of API requests
- Protection of API back-end infrastructures from low and slow attacks designed to exhaust resources (e.g., Slow Post, Slow Get)
- Definition of allowed API requests by key (quota for each key defined independently) for full control over consumption
- API onboarding using standard API definitions (Swagger/OAS and RAML)

API protections have become a critical part of web application security. You need a WAAP solution with robust API discovery, protection, and control capabilities to mitigate API vulnerabilities and reduce your surface area of risk.

FLEXIBLE MANAGEMENT 04

- Open APIs and the CLI to integrate security configuration tasks into CI/CD processes
- Real-time dashboards, reporting, and heuristics-driven alerting capabilities
- Integration with on-premises and cloudbased security information and event management (SIEM) applications
- Centralized user interface (UI) to access detailed attack telemetry and analyze security events
- Full staging environment and the ability to implement change control
- Self-tuning security protections that automatically adapt to your traffic
- Fully managed security services to offload or augment your security management, monitoring, and threat mitigation

You need simple and automated workflows to maximize your investment and improve operational efficiencies. Whether protecting new or changing applications, adopting new WAF rules, or extending protections to APIs, the process must be seamless and intuitive.

Akamai provides web application and API protection to the world's leading financial institutions. Every day, our global security research team gleans insight from millions of web application attacks, billions of bot requests, and trillions of API requests. This level of insight, coupled with advanced machine learning and threat research, allows us to constantly improve, catch new threats, and develop innovative capabilities.

Akamai's web application and API security solutions will secure your financial institution against the most advanced forms of web application, DDoS, and API-based attacks. Stay plugged in to our latest research by checking our Security Hub.

Akamai

Akamai powers and protects life online. Leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences — helping billions of people live, work, and play every day. With the world's most distributed compute platform — from cloud to edge — we make it easy for customers to develop and run applications, while we keep experiences closer to users and threats farther away. Learn more about Akamai's security, compute, and delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on Twitter and LinkedIn.