API

With Application Programming Interface (API) calls powering critical websites and apps, it’s essential that they are highly responsive and secure from attacks and other security threats. Your organization can do just that by taking advantage of unique, yet proven, technologies from Akamai.

Optimize Performance

Similar to web traffic, API call volumes can be unpredictable. Many enterprises use geographically diverse data centers or cloud providers to host their API infrastructure and redundant network architectures and components to try to combat inconsistent availability. However, traditional hardware load-balancing appliances alone can fall short, and data centers and cloud vendors are prone to unplanned downtime events. Plus, a peak event could overwhelm your infrastructure, resulting in a poor end-user experience.

Akamai has advanced methods to solve website performance challenges, and successfully applies them to improve API performance. Akamai’s unique solutions include:

- **API Acceleration.** Real-time data collected by Akamai selects an accelerated path between the client request hitting the Akamai Edge server and the origin.

- **API Caching.** Akamai can cache API responses at the Edge (even for mere seconds) to position them as closer to the calling API client (e.g., mobile device, tablet, kiosk, etc.) for offload. This keeps API requests off of the network.

- **API Compression.** By compressing 60–90% of the API responses that use text formats such as JSON or XML, Akamai can reduce payload size.

- **Transport-Layer Security (TLS) Termination at the Edge.** If the API requests are secure, the TLS handshakes can be negotiated at the Internet Edge instead of at the API origin, reducing the number of roundtrips required.

- **API Prioritization Cloudlet.** Akamai’s unique intelligence at the Edge can modulate the volume of requests that are sent to API-driven applications. At the same time, it can offer alternate static experiences to handle overflow traffic. This helps maintain availability of key applications, while providing visitors with a high-quality experience even when a site or application is under extreme load.
Address API Vulnerabilities

Just like web servers, API endpoints are exposed to attack risk from hackers and bots. In addition to malicious adversaries, APIs can be misused accidentally by calls that don’t fit into the use case envisioned when the API was created. As a result, API calls can become unintended conduits for a DDoS attack.

In fact, the complex and non-standard message formats of web and mobile API calls (i.e., JSON) make it hard for some security solutions to detect attacks within them.

Moreover, many developers make the mistake of assuming that since the API is masked behind another service (for example, a mobile application), security can be managed on the client side and relaxed on the API server. However, developers use standard HTTP methods to retrieve and manipulate resources, so typical web application vulnerabilities also apply to API requests. These requests are vulnerable to security threats throughout their life cycle due to an excessive rate of API calls, weak authentication and authorization, and other common practices.

These and other vulnerabilities in the API ecosystem have driven adversaries to shift their malicious activities from standard web applications to web APIs.

Akamai has deployed a three-tiered, cyclical approach for securing APIs:

1. **Define.** Use a positive security model to define how the API should be consumed.

2. **Enforce.** Use a negative security model to protect API endpoint web application attacks.

3. **Analyze.** Provide API-specific reporting for increased visibility into how end users interact with APIs.

For a deep dive into accelerating and securing your APIs, check out this on-demand webinar. For more on Akamai’s solutions, visit our API web page.

As the world’s largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai’s massively distributed platform is unparalleled in scale with over 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai’s portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, e-commerce leaders, media & entertainment providers, and government organizations trust Akamai please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 09/17.