Protecting your APIs

With API Gateway and Kona Site Defender
Kirsten Hunter

API Evangelist

5 years at Akamai
10 years working with APIs
Passionate about developer experience
Akamai’s API Management Platform

Security
KSD & Bot Manager Premier
Protection from adversaries trying to exfiltrate data or perform volumetric DDoS attacks

Governance
API Gateway
Ensure API consumers behave

Delivery
ION
Scalability you won’t outgrow

Protect the enterprise from attacks prior to invoking anything in a trusted zone.

Enforce runtime policies to drive consumption of business assets securely and easily.

Provide consistency of experience to more users with less infrastructure.

#EdgeWorld2019
APIs are a prime target

Hackers are constantly after your data
API Landscape
Attack Vectors

4X more credential stuffing attacks on APIs
Threats
The 4 Areas Where Your APIs are the Most Vulnerable

1. DDoS Attacks
2. Parameter Attacks
3. SQL Injection Attacks
4. Credential Stuffing Attacks
Distributed Denial of Service (DDoS) Attacks

Traditional request-rate-based controls are hard

Positive security / Input validation is hard

Understanding who and what to trust in a SaaS world is hard

Source: API & Security Trends for 2018

© 2019 AKAMAI

#EdgeWorld2019
Solution: Kona DDoS Defender

Kona DDoS Defender combines the automated DoS and DDoS protection capabilities of the globally-distributed Akamai Intelligent Platform with the security experience and expertise of Akamai’s 24x7 SOC.

STOP ATTACKS AT THE EDGE
- Defense with unmatched scale
- Automated mitigation capabilities for network and application-layer attacks
- Fully managed attack response from Akamai’s 24x7 SOC
- Security monitor for attack visibility

© 2019 AKAMAI

#EdgeWorld2019
Parameter Attacks

An important step for any resilient API implementation is to sanitize all incoming data to confirm that it is valid and will not cause harm.
Solution: Kona Site Defender

Positive and negative security models
Customers can define which types of requests and calls are allowed
Inspects the parameters of RESTful APIs against a whitelist of expected values
Inspects JSON body and path parameters for risky content
SQL Injection Attacks

Since your API is a programmatic interface, it’s important to guard against SQL injection or other attempts to convince your system to behave abnormally.

The vast majority of API attacks are SQL injection.

SQL query:
```sql
sql_query = "SELECT ItemName, ItemDescription FROM Item WHERE ItemNumber = " & Request.QueryString("ItemID")
```

Normal request:
http://www.estore.com/items/items.asp?itemid=999

SQL Injection:
http://www.estore.com/items/items.asp?itemid=999;DROP TABLE Users

76% of attacks are SQL injections
Solution: Akamai WAF

- Akamai WAF provides extensive protection against injection attacks with existing, out-of-the-box rules.
- Virtual patching can be automated and integrated.
- Client Reputation helps identify and block injection-based attacks from highly active bad actors.
- Injection-based attacks can also be further analyzed by the WAF with a Penalty Box Alert Mode.
Credential Stuffing Attacks

Credential stuffing attacks in 8 months

Source: Akamai SOTI 1Q 2019

DATA THEFT

CUSTOMER IDENTITY FRAUD

ACCOUNT TAKEOVER
Solution: API Gateway and Kona Site Defender

<table>
<thead>
<tr>
<th>Feature</th>
<th>API Gateway</th>
<th>Kona Site Defender</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication and authorization</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Quota Management</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Protection from malicious attacks</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>

© 2019 AKAMAI

#EdgeWorld2019
Launchpad Mission

Protect Your Site from Severe Security Threats based on the OWASP Top 10
How it works
API Gateway and Kona Site Defender

© 2019 AKAMAI

#EdgeWorld2019
Request Flow - With Akamai
API Gateway

Mitigate Security & Operational Risk

- Prevent unauthorized access
  - API key-based authentication
  - JSON Web Token validation
  - Secure API traffic with OAuth 2.0
  - Enforce business SLAs with global Quota limits
  - Throttle traffic to protect infrastructure (beta)
  - Identity Management (via Akamai Identity Cloud)

© 2019 AKAMAI
Scalability
- Gateway not locked into a DC or region
- Eliminate time penalties of auto-scaling
- No costly replication of infrastructure in multiple geographies
- No need to over-provision servers for biggest traffic day
- No single point of failure

Response Caching
- Cache RESTful responses at the edge to skip requests entirely
- GraphQL full query caching

CORS (Cross Origin Resource Sharing)
- Serve preflight headers from the edge to save round-trip and boost AJAX call performance
API Gateway

Developer Agility

Administrative APIs
- Integrate the Gateway into your CI/CD pipeline
- API catalog: developer.akamai.com/api

Command Line Interface
- Control of common Gateway functions without writing a line of code
- Script or automate repetitive or common tasks without writing to API

Swagger/RAML Import
- Use API definitions (Swagger, RAML, OpenAPI 3) already created to quickly and easily onboard APIs

© 2019 AKAMAI
Oauth authentication

Client → Authorization Request → Authorization Grant → Access Token ( & Refresh Token) → Resource Owner


Protected Resource

© 2019 AKAMAI

#EdgeWorld2019
JWT Authentication

JSON web tokens (JWT) settings

Credentials

Example connection credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client name</td>
<td>example-conn</td>
</tr>
<tr>
<td>Primary PSK</td>
<td>secret</td>
</tr>
<tr>
<td>Backup PSK</td>
<td>secret</td>
</tr>
</tbody>
</table>

JWT location

<table>
<thead>
<tr>
<th>JWT location</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>example-conn</td>
</tr>
</tbody>
</table>

JWT settings

Update JWT settings

Updates the JWT validation settings configured for an endpoint version and its associated resources.

PUT /api-definitions/v2/endpoints/(apiEndpointId)/versions/(versionNumber)/settings/jwt

Sample: /api-definitions/v2/endpoints/288595/versions/23/settings/jwt

Object type: JWTSettings

Download schema: jwt-settings-schema.json

Request Body:

```json
{
   "enabled": true,
   "settings": {
      "name": "auth",
      "validate": true,
      "required": false,
      "value": {
         "ala"
      },
      "type": "ARRAY"
   }
}
```
Throttling

- Critical component of API scalability
- Ensures fairness of access
- Control request rate per second to protect backend infrastructure
- Traffic is denied at Edge – does not transit to origin
- 3 levels of throttling:
  - API key
  - Endpoint/resource
  - HTTP method
- Not confined to a server, DC, or region
Kona Site Defender features

• Delivers the lowest false positives and false negatives to ensure access to legitimate users while keeping out threats.
• Continuously updates WAF rules based on 130 TB of threat data every day.
• Kona Site Defender detection logic is so advanced that it often catches zero-day attacks.
• Protects applications regardless of location.
• Realize a unified view of security posture.
• A user-friendly online portal based on a decade of real-world experience.
Kona Site Defender

Match Targets and Security Policy Order

This list runs in order, top to bottom. The last Match Target that matches an incoming request defines which security policy is applied. So order more specific match criteria later. API Match Targets take precedence over Website Match Targets. Learn more

Website Match Targets

1. Test for Launchpad [LNPD_76189]
   - Hostnames: ALL Hostnames
   - Directory: Match on all requests that end in a trailing slash

API Match Targets

There are no API match targets
## Application Security API and CLI

**Launchpad:** Vega $ akamai appsec help

**Usage:** akamai appsec <command> [options]

### Commands:
- `activate`  
  Activate a version.
- `activation`  
  Get activation status.
- `clone`  
  Clone a config.
- `configs`  
  List all available configurations.
- `enable-custom-rule`  
  Assigns an action (such as alert or deny) to an existing custom rule in a policy.
- `create-custom-rule`  
  Create a custom rule.
- `delete-custom-rule`  
  Delete a custom rule.
- `custom-rule`  
  Display contents of custom rule.
- `modify-custom-rule`  
  Update existing custom rule.
- `structured-rule-template`  
  Prints sample JSON of a structured custom rule.  
  [aliases: srt]
- `custom-rules`  
  List all custom rules.
- `export`  
  Export a configuration version.
- `add-hostname`  
  Add hostnames to selected list
- `selectable-hostnames`  
  List all selectable hostnames.
- `selected-hostnames`  
  List all currently chosen hostnames.
- `create-match-target`  
  Creates a match target.
- `modify-match-target`  
  Updates a match target.
- `match-target-order`  
  Change the match target sequence.
- `match-targets`  
  List all match targets.
- `policies`  
  List all security policies.
- `clone-policy`  
  Clone security policy.
- `version`  
  Read a config version
- `versions`  
  List all config versions
Summary

- APIs are heavily targeted by hackers
- Threats come in many flavors
- API management can help immensely
- Authentication is key
- Move your API protection to the edge to increase safety and performance
Thank you