Automated Safeguards for API Gateway

Amazon API Gateway is a fully managed service that makes it easy for developers to publish, maintain, monitor, and secure APIs at any scale. With Amazon API Gateway, you can quickly and easily create a custom API to your code running in AWS Lambda, EC2 instances, or any internet-accessible web service. And, to make it easy for you to use these APIs, Amazon API Gateway can generate client SDKs for a number of languages, including JavaScript, iOS, and Android.

Amazon API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management. Amazon API Gateway has no minimum fees or startup costs. You pay only for the API calls you receive and the amount of data transferred out.

With Amazon API Gateway, you only pay when your APIs are in use. There are no minimum fees or upfront commitments. You pay only for the API calls you receive and the amount of data transferred out. There are no data transfer out charges for Private APIs. However, AWS PrivateLink charges apply when using Private APIs in Amazon API Gateway. Amazon API Gateway also provides optional data caching charged at an hourly rate that varies based on the cache size you select. The API Gateway free tier includes one million API calls per month for up to 12 months. See the Amazon API Gateway pricing page for detailed pricing information.

Amazon API Gateway is a fully managed service that makes it easy for developers to publish, maintain, monitor, and secure APIs at any scale. With the proliferation of mobile devices and the rise in the Internet of Things (IoT), it is increasingly common to make back-end systems and data accessible to applications through APIs. Because so many applications use these APIs, and communities of developers rely on them, an increasing amount of time and effort is spent developing and managing APIs.

For a full description please see the API Gateway feature page.

Examples

Below are some examples of using API Gateway to connect to other AWS services with Automated Safeguards.

http://docs.aws.amazon.com/apigateway/latest/developerguide/integrating-api-with-aws-services-s3.html

https://aws.amazon.com/blogs/compute/using-amazon-api-gateway-as-a-proxy-for-dynamodb/

ClearDATA's Automated Safeguard for API Gateway ensures that any API Gateway stage that is deployed will have access logging enabled, and logging to an S3 bucket. In the event an API Gateway stage is deployed without access logging enabled, the Automated Safeguard will automatically enable logging.

Compliance Guidance

Customers may use Amazon API Gateway to process and transmit PHI. API Gateway passes all non-cached data through memory and does not write it to disk. Customers may use AWS Signature Version 4 for authorization with API Gateway. For more information, see the following:

- https://aws.amazon.com/api-gateway/faqs/#security
- https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-control-access-to-api.html

Customers may use the caching feature for API Gateway to process and transmit PHI as well. All data processed by API Gateway cache is encrypted both in motion and at rest, ensuring the data is compliant.

Audit Logging

The Automated Safeguard will create the appropriate IAM role and configure the appropriate API Gateway settings to enable access API logging to AWS CloudWatch.

The Automated Safeguard configures logging to use a Common Log Format and to ship logs to a CloudWatch Log Group for each API stage. The log format used by the Automated Safeguard is below

```
$context.identity.sourceIp $context.identity.caller  \
$context.identity.user [$context.requestTime] \
"$context.httpMethod $context.resourcePath $context.protocol" \
$context.status $context.responseLength $context.requestId
```

Remediation

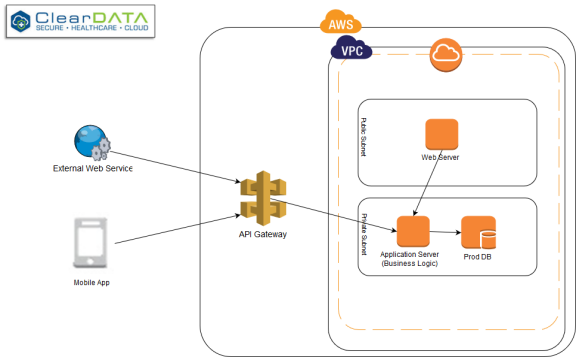
If access logs are not configured as part of the API Stage when it is deployed, the access logs are configured to log to CloudWatch.

Shared Responsibility

Customers may integrate with any service that is connected to API Gateway, provided that when PHI is involved, the service is configured consistent with the Guidance and BAA. For information on integrating API Gateway with back end services, see https://docs.aws.amazon.com/apigateway/latest/developerguide/how-tomethod-settings.html. Customers must also ensure that unencrypted protocols are never configured for use in API Gateway. Additionally, at no time should any API Gateway configurations contain any PHI/PII in the configuration itself.

Exclusion

Disabling automated remediation at done the API Stage level. Please contact ClearDATA Support to request that an exclusion be placed on the Stage.



RACI

Item	ClearDATA	Customer
Create API Gateways	C	RA
Deploy API Gateway stages	C	RA
Ensure Access Logging is enabled for all deployed stages	RA	IC
Configure and maintain all API Gateways	C	RA
Create client SDKs from API Gateway	C	RA
Configure & manage API Lifecycle Management	C	RA
Configure & manage API request authorization & verification	C	RA
All other API Gateway management	C	RA

Reference Architecture Diagram