Selecting the Right API Gateway to Protect Your APIs and Microservices

Published: 28 June 2018 **ID:** G00349440

Analyst(s): Mary Ruddy, Michael Isbitski

API gateways and microgateways play a key role in API and microservices architecture. They mediate access, monitor traffic and provide security features to reduce risk. This research gives technical professionals an evaluation of IAM, security and DevSecOps-enabling features from select vendors.

Key Findings

- API gateways have evolved significantly since our previous vendor survey in 2016. The market has progressed from relying primarily on monolithic API gateways, which are complex and often ill-suited to modern application architecture.
- A number of vendors have introduced microgateways, which have low latency, smaller size and scale to support a distributed, elastic, multi-instance architecture. Some vendors achieve this by reducing microgateway functionality more than others, including reducing IAM and security features that may not be needed because threats are mitigated at other layers of the network.
- A common deployment pattern is to use API gateways at the edge and microgateways between services for east-west or internal service-to-service traffic.
- Many API gateways are now more microservices- and DevSecOps-friendly, supporting increased automation and configurability. The trend is for microgateways to be containerized.

Recommendations

To deliver effective identity and access management capabilities for APIs and microservices:

- Identify the threats that you need protection from, and ensure that each threat is adequately mitigated using an appropriate tool. For some cases, an API gateway or microgateway can provide sufficient mitigation. Otherwise, leverage separate systems or protections within the broader enterprise architecture for comprehensive mitigation.

- Wherever practical, choose API gateways and microgateways that can be managed via the same administrative user interface, when you need multiple gateways to meet multiple use cases (e.g., cloud, on-premises, APIs and microservices).
- Use the data in The Details section to confirm support for specific IAM and security protection features that you require of an API gateway or microgateway. Examples include support for throttling in API gateways or microgateways, or support for DDoS protection on API gateways.

Table of Contents

List of Tables

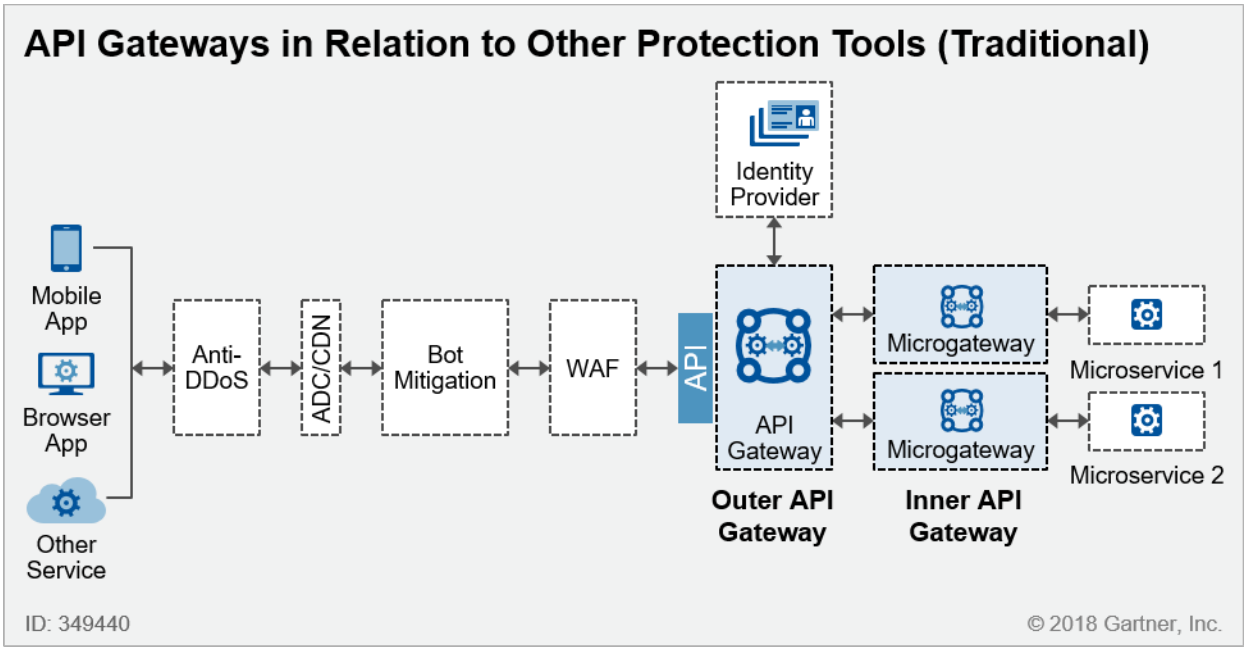
List of Figures

Analysis

Organizations developing and maintaining their own APIs need to manage those APIs, control access to them, and protect them from cyberthreats and misuse. APIs and the credentials used to access them are common targets of attack. Technical professionals in charge of protecting APIs should adopt the appropriate API life cycle management tools — including API gateways and/or microgateways — as part of their overall API protection approach. (See also "A Guidance Framework for Evaluating API Management Solutions.")

API gateways and microgateways are one part of an overall protection architecture. For the purposes of this analysis, protection consists of identity and access management (IAM) and security. Figure 1 depicts one example of a traditional relationship between API gateways and other application architecture components. In addition to an API gateway and/or microgateway, appropriate protection usually includes a separate IAM system. It may also include distributed denial of service (DDoS) protection, bot mitigation, web application firewalls (WAFs), application delivery controllers (ADCs), content delivery networks (CDNs), and so on. An analysis of web application and API attacks (i.e., the threats), as well as the mitigating technologies, is provided in "Protecting Web Applications and APIs From Exploits and Abuse."

Figure 1. Example Relationship Between API Gateways and Other Protection Tools (Traditional)



Source: Gartner (June 2018)

API gateways provide a crucial layer of runtime API mediation. An "enterprise," "edge" or "outer" API gateway protects north-south traffic. The primary role of a microgateway, or "inner" gateway, is to manage service-to-service communications (i.e., east-west interservice traffic between microservices).

Microgateways are lightweight, distributed API proxies that enforce policies at, or near, service endpoints. Microgateways support a limited set of capabilities compared with enterprise API gateways or full life cycle API management solutions. Key microgateway capabilities include last-mile authentication and authorization, traffic management, monitoring, and scriptable policy configurations managed under source control.

For an API gateway to be considered a microgateway, it must be suitable for deployment as an inner gateway paired with a microservice instance. Thus, it must:

- Be containerized or container-ready
- Have no limit on number of instances
- Incur no (or very low) license fees for additional instances
- Provide low latency
- Have a small footprint
- Be amenable to centralized and automatic administration

Note that a couple of vendors (Kong and Red Hat) have offerings that can be deployed as both API gateways and microgateways. These vendors have managed to squeeze robust functionality into an offering that can be used as either an inner or an outer gateway. There is a trend now toward lower-footprint gateways that have more flexible deployment options.

Use cases and requirements for API gateway deployments vary widely. The range of needs continues to expand, and enterprises may require support for any of the following:

- External and internal APIs
- Traditional APIs
- Miniservices
- Microservices
- Web or mobile application use cases
- Service-to-service use cases
- Internet of Things (IoT) use cases

For example, some enterprises need edge gateways that can interoperate with legacy IAM systems and APIs, while others are concerned only with protecting new microservices deployments.

Best practices for using microgateways and protecting microservices are still emerging. An increasingly common approach with microservices architectures is to deploy a microgateway as a sidecar proxy, which requires a microgateway that is lightweight and extremely fast. As microservices tooling becomes more standardized, some organizations are developing service mesh architectures. A service mesh supports internal communication and dependency management between microservices. For example, several of the microgateway vendors are

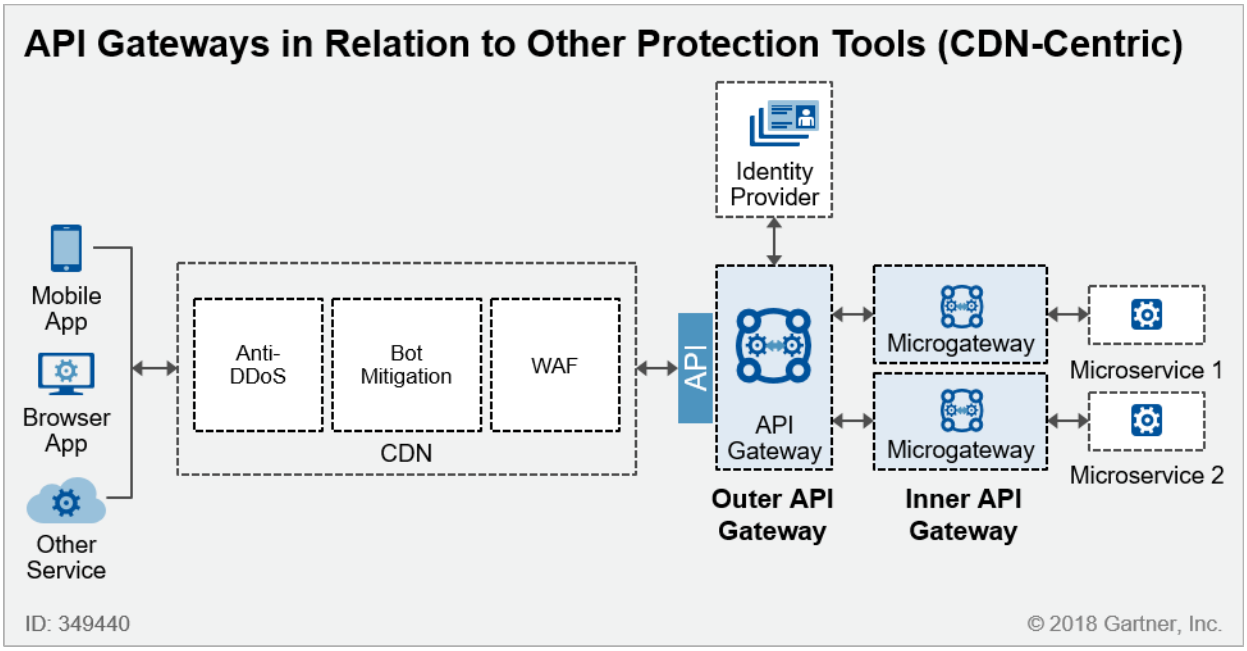
collaborating on the open-source service mesh project Istio. For deeper coverage of service mesh architecture, see "Selecting a Cloud Platform for DevOps Delivery With Microservice Architecture" and "Assessing Microservices for Agile Application Architecture and Delivery."

Role of API Gateways in a Broader Enterprise Protection Architecture

A complete enterprise web application architecture is a combination of one or more application-layer components, including ADCs, WAFs, API gateways, HTTP servers, application servers, database servers and IAM systems. For cloud-hosted or internet-facing applications, a CDN is also often used. The CDN provider is itself a collection of many globally distributed data centers, or points of presence, running load balancers, content caches and content accelerators.

Figure 1, above, is not the only possible approach to an enterprise protection architecture. Your organization's architecture may utilize additional layers of proxies, load balancers or network paths. A CDN-centric approach, where the CDN provides multiple integrated protection capabilities, is depicted in Figure 2.

Figure 2. Relationship Between API Gateways and Other Protection Tools (CDN-Centric)



Source: Gartner (June 2018)

Like an ADC or WAF, an API gateway is a type of reverse proxy that can also fill the role of certain security functions. The question is often whether an API gateway is the most effective enforcement point for security controls. API gateways are implemented to facilitate API communication and traffic management. Any custom message handling can hinder performance. The accepted security function of an API gateway, in most cases, is to enforce IAM and API management policies. A WAF,

on the other hand, is tasked predominantly with exploit mitigation for all HTTP traffic, regardless of whether that traffic originates from a traditional web application or a web API.

Cloud-delivered API gateways can often provide a wider range of capabilities by virtue of virtualization, cloud scalability and bundling of services. Moreover, cloud service providers (CSPs) will often provide tighter or simplified integration within their ecosystem, as demonstrated by Amazon Web Services (AWS) and Microsoft Azure with their respective API gateway and WAF offerings. However, with cloud services, latency may still be a factor. In the earlier days of the Amazon API Gateway, there was reported latency during instantiation and during regular operation. AWS has since remedied the problem and improved performance. However, the variability of cloud service performance and latency may be a deciding factor to select an on-premises API gateway as opposed to a cloud-based one.

Organizations deploying cloud-based applications may also look to leverage function platform as a service (fPaaS) to handle some security functions. For example, organizations may use fPaaS functions to dynamically encrypt data — separately from the API gateway, but as part of an API communication. However, this approach can raise similar concerns over cloud performance and latency. Completion of an overall API request and response may be dependent on the startup latency of a function within the fPaaS platform (e.g., AWS Lambda, Azure Functions or Google Cloud Functions). For advanced security functions, activity will also likely need to be blocking, which can reduce the overall performance and round-trip response of the API communication.

Open Authorization (OAuth) and OpenID Connect (OIDC) are the IAM standards used to protect modern APIs. Some organizations also have existing services protected by Security Assertion Markup Language (SAML). The specific OAuth/OIDC IAM requirements vary widely by use case. APIs may be accessed via web browsers, invoked by native mobile apps or used for service-to-service interactions. An access token may be generated by an identity provider in an external IAM system. That token may then be forwarded to an outer gateway to control access and to pass attributes used for fine-grained authorization. For more background on IAM best practices for APIs and microservices, see:

- "Modern Identity and APIs: Mobile, OpenID Connect, OAuth, JSON and REST"
- "Best Practices for Using the Evolving OAuth 2.0 Framework"
- "Single Sign-On in Native Apps and Modern Web Apps"
- "Building Identity Into Microservices"

As organizations understand and prioritize their specific protection requirements, they can utilize the data in this research to identify the offerings that best align with their needs. Note that, although API gateways and microgateways utilize a number of standards, the configuration mechanism for each vendor is different. Organizations should look to minimize the number of API gateway and microgateway configuration management mechanisms that they use.

This document compares the identity and security capabilities available from a number of API gateways and microgateways. It also includes information about some basic DevSecOps features that security and identity professionals consider. It is not a complete evaluation of all the capabilities

available in full life cycle API management solution. For example, it does not discuss the specific features found in API developer portals, the design of configuration interfaces, or DevOps details.

Comparison

There are many providers of API gateways and microgateway solutions. This assessment focuses on the following 13 vendors and their offerings (listed in alphabetical order by vendor, with offerings ordered sequentially):

- Amazon API Gateway
- Apigee Edge 17.12.13
- Apigee Edge Microgateway 2.5.8
- Axway API Gateway 7.5.3
- CA Technologies API Gateway 9.3
- CA Technologies Microgateway 1.0
- IBM DataPower Gateway 7.6
- IBM API Connect Microgateway
- Kong Enterprise Edition 0.30
- Microsoft Azure API Management
- MuleSoft Mule 3.9.0 (currently 4.1.2; note that Salesforce acquired MuleSoft in May 2018)
- NGINX Plus R15
- Red Hat 3scale APIcast API gateway 2.1
- Software AG webMethods API Gateway 10.1
- TIBCO Software API Exchange Gateway 2.3
- TIBCO Mashery Enterprise (TIBCO Mashery Local is 4.2)
- TIBCO Project Mashling
- WSO2 API Manager/WSO2 API Cloud 2.1.0 (currently 2.2)
- WSO2 API Microgateway 2.1.0

Versions are included, where provided by the vendor. In some cases, such as for open-source software (OSS) or cloud services, the vendors did not provide version numbers for their API gateways or microgateways.

This list is not exhaustive. The market for API gateways and microgateways is dynamic. Other API gateway and microgateway vendors not assessed in this research include, but are not limited to, Akana, Cloud Elements, Cloudentity, Dell Boomi, digitalML, Kony, Nevatech, Oracle, SAP, Sensedia, SmartBear, Torry Harris Business Solutions (THBS), Tyk and Traefik. Vendors included in this comparison consist of all of the vendors in the most recent Leaders quadrant of the Gartner "Magic Quadrant for Full Life Cycle API Management." In addition, we included some of the vendors positioned near the boundaries of the Leaders quadrant, because we frequently receive inquiries about them. We also included NGINX, an open-source web program on which several other offerings are based. Note also that some vendors declined to participate in the survey on which this research is based.

Comparison Methodology

This comparison assessment is based on a fixed set of criteria. Gartner's defined set of criteria is based on the following:

- The topics normally discussed in client inquiry calls regarding security and IAM API management.
- The factors Gartner believes should be important for organizations protecting APIs and microservices.

Gartner assessed all the defined criteria consistently and methodically across all the solutions compared, and each solution has been assessed against the same set of criteria.

Each criterion is made up of one or more attributes. Each attribute, as described in this assessment, has been examined separately, but all the attributes of a single criterion translate to a single rating. The criteria are evaluated on the following Gartner-defined scale:

1 = None

2 = Via customization

3 = Via integration with any other product for non-IAM features, or via integration with another offering by the same vendor for IAM features (all gateways can integrate with other IAM systems via identity standards)

4 = Yes

* = Is on roadmap

The comparison in Figure 3 consists of five categories (columns). The first two categories, API Gateway and Microgateway, are based on a single feature. For these two columns, the ratings vary slightly from the scale above. Only two values are possible: 1 (No) or 4 (Yes). An asterisk indicates that the feature is on the vendor's roadmap.

For the other three columns in Figure 3, the ratings are composite scores. Each score represents the average of a number of individual feature ratings. Information on the features we evaluated to generate these three composite scores is provided in The Details section below. See the following subsections:

- IAM Score Details
- Security Score Details
- DevSecOps Enablement Score Details

The Details section also includes a Licensing Options section with information on how the offerings are licensed.

Figure 3 provides comparison data for all the assessed solutions.

Figure 3. Comparison for API Gateways

Comparison of API Gateway Protection Features

Offering	API Gateway	Micro-gateway	IAM	Security	DevSecOps Enablement
Amazon API Gateway	4	1	2	3	3
Apigee Edge	4	1	4	4	4
Apigee Edge Microgateway	1	4	2	3	4
Axway API Gateway	4	1	3	3	4
CA Technologies API Gateway	4	1	4	4	4
CA Technologies Microgateway	1	4	2	4	3
IBM DataPower Gateway	4	1	4	4	3
IBM API Connect Microgateway	1	4	2	2	3
Kong Enterprise Edition	4	4	4	3	4
Microsoft Azure API Management	4	1	3	3	3
MuleSoft Mule	4	1	3	4	4
NGINX Plus	1	4	2	3	3
Red Hat 3scale APIcast API Gateway	4	4	3	4	4
Software AG webMethods API Gateway	4	4*	3	4	3
TIBCO API Exchange Gateway	4	1	3	2	4
TIBCO Mashery Enterprise	4	1	2	3	4
TIBCO Project Mashling	1	4	1	3	3
WSO2 API Manager/API Cloud	4	1	3	4	4
WSO2 API Microgateway	1	4	3	4	3

Key:
Fill color correlates to the offering's strength in each listed criterion.
For the API Gateway and Microgateway columns:
1 = No
4 = Yes
The other columns are an average of individual feature ratings of:
1 = None
2 = Via customization
3 = Via integration with any other product for non-IAM features, or via integration with another offering by the same vendor for IAM features (all API gateways can integrate with other IAM systems via identity standards)
4 = Yes
* Is on roadmap.
ID: 349440

Source: Gartner (June 2018)

Each solution is described in more detail in the Solution Assessments section.

Solution Assessments

Amazon API Gateway

The Amazon API Gateway is primarily used to integrate with and leverage a wide range of other AWS services, including Lambda, AWS's fPaaS. The identity and access management capabilities are supported via integration with multiple AWS products:

- Amazon Cognito for OAuth authorization server support, OpenID provider support and SAML service provider support
- AWS IAM for SAML identity provider support
- Lambda authorizers

Security functionality is also spread across multiple AWS products. To achieve the full range of security functionality, you would need to use other paid AWS services, including:

- AWS WAF for exploit mitigation. Out of the box (OOTB) functionality and rules are more basic, but this service may be sufficient for some simpler use cases. AWS has also established a marketplace where, for an additional cost, customers can subscribe to managed WAF rule sets from vendors such as F5, Fortinet and Imperva.
- Amazon CloudFront Field-Level Encryption to encrypt API message data.
- Amazon GuardDuty, launched November 2017, for behavior analysis and threat detection.

Strengths

- Amazon API Gateway is attractive for AWS customers deploying services in AWS, including customers deploying to AWS serverless back ends or traditional compute back ends.
- The Amazon API Gateway offering is highly programmable and automatable, making it suitable for organizations applying DevSecOps principles. (Of course, to automate configuration of the gateway and integrate it with other AWS services effectively, such organizations must have the necessary engineering resources.)
- Organizations that are already using AWS and the other services that Amazon API Gateway leverages will find them familiar.
- Amazon API Gateway integrates with Red Hat 3scale API Management for policy enforcement and monitoring across both the Amazon and Red Hat gateways.

Weaknesses

- Amazon API Gateway is available only as a cloud service. There is no support for on-premises gateways to reduce latency in circumstances where users and APIs are all on-premises.

- If organizations are not already familiar with the AWS features that Amazon API Gateway leverages, they may find using the multiple configuration interfaces difficult.
- AWS does not support OAuth natively. OAuth can be configured using Cognito, but this process involves a lot of effort and complexity relative to the other infrastructure as a service (IaaS) platforms, which support OAuth natively for IaaS API access.
- Native security with Amazon API Gateway is limited to certain traffic management functions. Other security functions require use of AWS services or external capabilities.
- AWS does not currently offer specific bot mitigation capability, either natively or through integration. However, Amazon GuardDuty can uncover some bot activity and abuse through behavior analysis.

Apigee Edge and Apigee Edge Microgateway

Google acquired Apigee in 2016. Apigee was founded in 2004. The Apigee Edge API management platform includes the API runtime/gateway and developer portal. It optionally includes monetization and Apigee Sense, a cloud-only analytics offering. Apigee Edge Microgateway is bundled with Apigee Edge.

The API gateway in the Apigee Edge platform provides a wide range of IAM support. Apigee's strong focus on scalability, as well as its focus on support for automation within continuous integration/continuous deployment (CI/CD) pipelines, makes it useful for organizations employing DevSecOps practices.

Bot mitigation and behavior analysis are provided separately with Apigee Sense. Tuning of Apigee Sense requires working with Apigee managed services, though Apigee is exploring the use of machine learning as part of its product roadmap to serve this purpose. Data tokenization capability in Apigee Edge, if needed, is provided through Google Cloud Data Loss Prevention (DLP) API.

Strengths

- Apigee-managed cloud service deployment enables organizations to use the API runtime components in multiple geographic cloud regions that they select.
- The API gateway in the Apigee Edge platform is one of the highest-scoring offerings in the area of IAM. Its security token service (STS) is particularly flexible, and its support for automation of SOAP-to-REST and REST-to-SOAP translation is particularly nuanced. Apigee Edge is also one of the highest-scoring solutions in the area of security. It provides a full range of capabilities natively or in tandem with Apigee Sense.
- Apigee provides both software and cloud service options, including containerized deployments.

Weaknesses

- Bot mitigation and behavior analysis require additional Apigee Sense licensing. When combined with Apigee Sense for bot mitigation, Apigee Edge moves ahead of many of its API gateway competitors. However, Apigee Sense does not provide the level of functionality found in

dedicated bot mitigation solutions. Apigee aggregates data from other customers to form the bot mitigation rules, and a customer is limited to enabling or disabling these rules in Sense. There is no ability to customize rules to mitigate attacks from advanced bot attacks or API abuse cases.

- The Apigee Edge for Private Cloud on-premises option has no ability to add Apigee Sense.
- Apigee Edge Microgateway does not offer data security features natively. Blocking of messages with sensitive data, data masking, tokenization and encryption all require custom code or plug-ins.

Axway API Gateway

Axway is an established API gateway vendor, having acquired Vordel in 2012. Axway API Gateway is the base runtime gateway. The Axway API Manager provides self-service API registration, consumption and administration capabilities on top of the API Gateway. The new Axway AMPLIFY API Central Service, introduced in 2017, is a public cloud service that enables organizations to manage a central catalog of APIs and to deploy microgateways (based on NGINX). Axway API Gateway is available either as software that can be containerized or as a cloud service, but it is not designed for microgateway deployment architectures.

Axway offers content inspection and threat protection via customizable XML and JavaScript Object Notation (JSON) validation. Axway also offers more advanced capability through an embedded ModSecurity module. In addition, the product supports integration with antivirus solutions to perform malware analysis of API traffic. The gateway can also integrate with Check Point Software Technologies' firewalls via the Open Platform for Security (OPSEC) framework.

Strengths

- Axway is targeted at large enterprise organizations that need to support legacy IAM environments.
- Axway supports a wide range of third-party single sign-on (SSO) cookies.
- Axway is strong in B2B use cases that involve Secure FTP (SFTP) file transfer.

Weaknesses

- Axway API Gateway is not suitable for managing interactions between microservices. The AMPLIFY API Central service was not evaluated as part of this research.
- Although Axway provides all the basic OAuth and OIDC features, it lacks support for many recent extensions and for some of the newer data store formats, such as Microsoft Azure Active Directory Graph API.
- Axway does not provide DDoS protection, bot mitigation or behavior analysis, either natively or via integration.

CA Technologies API Gateway and Microgateway

CA Technologies acquired Layer 7 in 2013, and has continued to invest in tools to automate the management and creation of APIs. CA API Gateway and CA Microgateway are part of a larger suite of products that includes CA Mobile API Gateway, CA API Developer Portal and CA API Management SaaS. (Version 1.0 of CA Microgateway was released in September 2017.) CA API Gateway is available either as software that the organization can install or as a cloud service, and both gateways are available as Docker containers.

CA provides a complete set of security functionality natively in both the API gateway and the microgateway. In the areas of traffic management, content inspection and threat protection, and data security, there is almost complete feature parity between the gateway and microgateway, with data encryption being the one exception. Exploit mitigation in the products is also extensive, given CA's pedigree. Both products can be integrated with numerous antivirus solutions via Internet Content Adaptation Protocol (ICAP) support, and current supported vendor integrations include McAfee, Sophos and Symantec. CA also has an extensive list of security certifications, including Federal Information Processing Standard (FIPS) 140-2, which may make it appealing to organizations seeking a product that meets compliance and regulatory requirements. Moreover, in April 2017, CA acquired Veracode, a provider of application security testing (AST) services. Veracode's AST technology could be beneficial to the CA gateway products in the areas of exploit mitigation, bot mitigation and behavior analysis.

Strengths

- CA API Gateway is one of the highest-scoring offerings in the area of IAM. It provides more complete support for OAuth and OIDC than most. For example, it supports more of the newest OAuth extensions than most of the other gateway offerings. These extensions can be important for protecting APIs from threats, such as compromised access credentials, and for streamlining operations processes. The CA API Gateway's STS also supports more token formats than most of the other STSs.
- CA API Gateway is particularly strong in support for non-HTTP communication protocols.
- CA API Gateway is one of the highest-scoring solutions in the area of security. It provides a full range of capabilities natively, with the exception of DDoS protection.
- CA API Gateway offers advanced exploit mitigation and behavior analysis, differentiating it from most of the API gateway competitors. The technology is sometimes branded as "XML firewall" or "API firewall." It provides the ability to define custom threat protection rules or "assertions" to detect and block API exploits.

Weaknesses

- CA Microgateway is relatively new and not yet proven in large deployments.
- CA API Gateway doesn't support some of the newer data access mechanisms, such as Microsoft Azure Active Directory Graph API and GraphQL.

- Though CA offers extensive DoS protection, DDoS protection is not offered natively or through integration with another service.

IBM DataPower Gateway and API Connect Microgateway

IBM acquired the StrongLoop microgateway in 2015. IBM DataPower Gateway and IBM API Connect Microgateway are available separately or as part of IBM API Connect (for full API life cycle management). IBM API Connect Microgateway is built using Node.js, which allows for easy integration of node modules. Specifically, several modules are available that can be used as part of the microgateway to support SAML and OIDC requirements. The microgateway leverages NGINX for reverse proxy, and Redis for multi-instance rate limiting. IBM supports the microgateway via contributions to its open-source code repository. Although the codebases of the two gateways are different (partially due to heritage), the UI is unified.

IBM DataPower Gateway provides strong exploit mitigation and a range of data security functions natively. A FIPS 140-2-certified hardware security module (HSM) is also offered as an option for key management. In addition, IBM DataPower Gateway provides extensive DoS protection for single-message and multimessage XML. Bot mitigation in DataPower Gateway is offered through a partnership with Ping Identity (formerly Elastic Beam). DDoS protection is offered through a partnership with Cloudflare.

Strengths

- IBM DataPower Gateway is one of the highest-scoring offerings in the area of IAM. For example, its STS supports a particularly wide range of token types and proprietary session cookies.
- IBM provides customizable JSON and XML threat protection, along with prebuilt protections for cross-site scripting (XSS) and SQL injection.
- IBM DataPower Gateway is the only offering surveyed that provides a purpose-built, physical network appliance form factor, where the hardware, the OS and the API runtime processing stack are built from the ground up with an emphasis on security.

Weaknesses

- IBM API Connect Microgateway does not natively provide some of the traffic management, content inspection and threat protection, or data security capabilities measured in this analysis. It requires custom JavaScript to provide some of the capabilities.

Kong Enterprise Edition

Kong (formerly Mashape) was founded in 2010 and offers an open-source API and microservices management solution. Kong is based on NGINX. Kong Enterprise Edition (EE) is targeted at medium- to large-scale global organizations. It includes the API gateway, Kong Dev Portal and Kong Vitals (for analytics and monitoring). Unlike with other vendors, these features are not sold separately, and they don't require independent installation — they leverage a single, unified code

base. Kong Community Edition (CE) is free open-source software, but it doesn't include all of the functionality in Kong EE. For example, Kong CE lacks a web-based administrative UI and role-based management capabilities.

Kong EE satisfies most security functions natively, through customization or through integration with other capabilities. The exception is DDoS, where no protection is offered. The vendor partners with Wallarm, a WAF vendor, for exploit mitigation, and Ping Identity (formerly Elastic Beam), an API security vendor, for bot mitigation. Data security requires the use of custom plug-ins.

Strengths

- Kong was developed to address the microservices use case and supports DevSecOps deployment scenarios.
- Kong has a single code base for its gateway, which can be deployed as either an API gateway or a microservices gateway.
- Kong supports most of the newer OAuth/OIDC extensions and has the broadest support for OAuth/OIDC flows.
- Kong supports context-based authentication, sometimes referred to as "adaptive access."

Weaknesses

- Kong traditionally was not available as a service. However, Kong Cloud is now in beta.
- Kong does not support SAML, translation between XML and JSON, or translation between SOAP and REST. Thus, it is not suitable for organizations with a traditional IAM infrastructure.
- Kong does not provide DDoS protection natively or via integration.

Microsoft Azure API Management

Microsoft acquired Apiphany in 2013. Microsoft Azure API Management includes the API gateway and developer portal. The Azure portal is the administrative interface. The Azure API Management offering can leverage other Azure platform capabilities. For example, Azure Logic Apps can be used to manage orchestration policies that can then be integrated into Azure API Management. Monitoring and alerting can also be managed through the Azure portal.

Like other CSPs, Microsoft Azure spreads security functionality across multiple products. To obtain all protection capabilities, you would need to pair Azure API Management with other Azure services, such as Azure DDoS Protection, Azure Application Gateway with WAF, and Azure Active Directory (Azure AD). Microsoft also partners with Barracuda Networks, a WAF vendor, for advanced exploit mitigation. Azure Application Gateway is a multipurpose ADC delivered as a virtual appliance. The WAF feature set is based on ModSecurity and on the Open Web Application Security Project (OWASP) ModSecurity Core Rule Set (CRS). Microsoft is also taking a more holistic approach to security with Azure Security Center, its central console for native Azure functions and some third-party capabilities.

Strengths

- Microsoft Azure API Management's premium tier supports deploying gateways across different Azure data centers worldwide.
- Microsoft Azure API Management provides broader support for context-based authentication than most offerings.
- Microsoft Azure API Management has good ease of use.
- Microsoft takes a unique approach to exploit mitigation via integration with the Azure Application Gateway with WAF. This approach can be appealing to organizations looking for exploit mitigation that is easy to configure and maintain. Customization is currently limited to toggling of individual CRS rules, but custom rule creation may be added in future releases. For advanced exploit mitigation, Microsoft partners with Barracuda Networks.

Weaknesses

- Microsoft Azure API Management is available only as a cloud service, not as software.
- Microsoft Azure API Management supports only HTTP/HTTPS protocols.
- Microsoft does not offer bot mitigation or behavior analysis with Azure API Management.
- Although the gateway can block messages with sensitive data or mask data, it does not include an option for data tokenization.

MuleSoft Mule

Salesforce acquired MuleSoft on 2 May 2018. MuleSoft provides support for a wide range of deployment options. Mule is the runtime engine of the Anypoint Platform and can be deployed as an API gateway.

With the launch of Anypoint Edge Security in February 2018, MuleSoft provides one of the most complete sets of security capabilities natively. Anypoint Edge Security is included in standard subscriptions. MuleSoft is lacking only in the area of bot mitigation. However, it does provide in-house behavioral analysis with the Anypoint Platform, which aggregates data from other clients of the cloud service platform and from threat intelligence feeds to detect threats that may include malicious bots. Mule can also be run in a FIPS 140-2-compliant mode.

Strengths

- MuleSoft provides stronger-than-average support for non-HTTP/HTTPS protocols.
- MuleSoft provides one of the most complete feature sets for security among the competitors, and it does so natively.

Weaknesses

- MuleSoft relies on third parties for OpenID provider support.
- MuleSoft supports only a couple of the OAuth/OIDC extensions natively.
- MuleSoft lacks specific bot mitigation capability. However, the Anypoint Platform does provide behavior analysis that can be useful for identifying potentially malicious bots.

NGINX Plus

NGINX is a high-performance, multipurpose application-layer software that can fulfill a variety of roles, including ADC, HTTP server, WAF, and API microgateway. Modularity in the design allows for custom coding or third-party plug-ins. A number of other nonsecurity and security vendors, including IBM, Kong and Red Hat 3scale, have extended NGINX in other application-layer solutions.

With respect to security, NGINX Plus provides integrations with certified module vendors to extend its security capabilities. These include integrations with Stealth Security and Signal Sciences for bot mitigation, as well as integrations with Signal Sciences, Trustwave ModSecurity and Wallarm WAF for exploit mitigation. On top of the NGINX Plus licensing, NGINX charges additional fees for the following:

- NGINX WAF module
- Trustwave SpiderLabs commercial ModSecurity rule set

DDoS protection is offered through Cedexis (now part of Citrix).

Strengths

- NGINX provides its core functions in a very efficient manner.
- NGINX supports a number of non-HTTP/HTTPS message formats.

Weaknesses

- NGINX provides very little IAM functionality natively, although it does support context-based authentication.
- NGINX doesn't provide XML-to-JSON translation or SOAP-to-REST translation.
- NGINX is lacking in the area of data security, but capabilities can be either built with custom Lua code or added via integrations with third-party products. There were no certified modules at the time of this analysis.
- With the exception of traffic management, most of the security features measured in this analysis are not native to NGINX Plus. They will require additional licensing from NGINX or some of its certified module vendors.

Red Hat 3scale APIcast API Gateway

Red Hat acquired 3scale in 2016. 3scale was founded in 2007. The Red Hat 3scale API Management platform is composed of two functional areas:

- APIcast API gateway (policy enforcement)
- API manager (policy decisions and community management)

Each can be deployed either on-premises or in the cloud. The Red Hat 3scale API Management platform leverages NGINX as its core software and augments that foundation with significant additional functionality. The APIcast API gateway component is currently open source. There are plans to open-source the rest of the solution later in 2018.

Red Hat supports a range of newer deployment topologies, including both containerized and cloud service options. For example, its API gateway can be deployed in a sidecar pattern (deployed in a container adjacent to the main microservice container) as part of a service mesh.

Red Hat provides almost the complete range of security capabilities, either natively or via integration with other tools. This includes the NGINX WAF module for exploit mitigation and Red Hat Fuse for data security. Red Hat Fuse can transform message data. This capability can be used to provide data security features like data masking and tokenization. XML and SOAP support is also provided via Red Hat Fuse. In addition, Red Hat partners with Ping Identity (formerly Elastic Beam) to provide advanced exploit mitigation and bot mitigation.

Strengths

- Red Hat 3scale was architected from the beginning to support microgateway deployments. Therefore, it leverages a common code base for both API gateway and microgateway deployment scenarios.
- Red Hat 3scale API Management platform can integrate with Amazon API Gateway to provide enhanced policy enforcement and monitoring across both the Amazon and Red Hat gateways.
- Red Hat 3scale APIcast API gateway provides a relatively complete set of IAM functionality. However, it lacks support for some of the most recent OAuth extensions and for some legacy protocols.
- Red Hat 3scale APIcast API gateway provides almost all security capabilities natively or via integration with other tools.

Weaknesses

- Red Hat 3scale APIcast API gateway does not support context-based authentication when used as an identity provider (which is consistent with Red Hat's recommendation to use a third-party identity provider).
- Organizations looking to mediate internal employee access to APIs should note that the Red Hat 3scale APIcast API gateway STS doesn't support Kerberos.

- Red Hat 3scale APIcast API gateway does not provide DDoS protection natively or through partnership with another vendor. Organizations would need to select a separate vendor offering to mitigate risk of DDoS attacks against web APIs.

Software AG webMethods API Gateway

Software AG webMethods API Gateway is part of Software AG's API Management Platform, which also includes:

- webMethods API Portal
- CentraSite (a registry and repository for APIs and other related services and assets)
- webMethods CloudStreams (which monitors and controls the consumption of APIs)

Software AG is limited in the area of security. It provides most of the basic traffic management functions, but lacks DDoS protection. It provides a threat protection layer within the API gateway runtime that allows for creation of custom filters, rules and behaviors that can be useful for exploit mitigation. The gateway can also be integrated with antivirus solutions via ICAP. Additional security functions, such as behavior analysis, data tokenization and data encryption, are provided via the webMethods Integration Server product.

Strengths

- Software AG's enterprise service bus heritage enables it to support a wide range of existing infrastructure (its STS accepts Kerberos tickets).
- Software AG's webMethods Microservices Container offering can be used to reduce the footprint of the gateway. (Software AG also supports containerization using Docker, via a single command.) Software AG plans to offer an additional microgateway component in 2018.
- Software AG provides consumption management for APIs to help organizations minimize usage of expensive third-party services.

Weaknesses

- webMethods API Gateway doesn't support some of the newer data access mechanisms, such as Microsoft Azure AD Graph API and GraphQL.
- Software AG webMethods API Gateway requires the use of webMethods Integration Server and additional customization for some security use cases.

TIBCO API Exchange Gateway, TIBCO Mashery Enterprise and TIBCO Project Mashling

TIBCO Software acquired Mashery in 2015. TIBCO refers to the Mashery cloud service gateway as the API Traffic Manager. TIBCO has extended its Mashery cloud service offering by adding Mashery Local for on-premises gateway deployments. Mashery Local's gateway comes with support licenses for Mashling, TIBCO's open-source microgateway. TIBCO continues to offer its API

Exchange Gateway for use cases that are on-premises only, or that require additional security features. The TIBCO Mashery developer portal works with both Mashery and the API Exchange Gateway.

TIBCO's security capabilities are strongest with the API Exchange Gateway. Although API Exchange Gateway lacks DDoS protection, bot mitigation, behavior analysis and data tokenization, it satisfies the other security criteria. It provides prebuilt policies for mitigation of XML and SQL injection. It also integrates with antivirus solutions via ICAP.

Mashery Enterprise maintains most of the security capability of the on-premises API Exchange Gateway, but also adds DDoS protection by virtue of being a cloud service. Mashling lacks most of the security capabilities out of the box, but it is extensible by design. Customers can create Go-based "recipes" to extend functionality, including security functions. TIBCO lacks bot mitigation and behavior analysis across all products, but TIBCO's product roadmap initiative to leverage machine learning could address these issues.

Strengths

- TIBCO Mashery API Control Center customers can choose, on an endpoint-by-endpoint basis, whether to route traffic via the cloud service API Traffic Manager or via an on-premises API Exchange Gateway. They can also govern where the API traffic needs to be routed to, depending on their organization's georouting and edge-caching requirements.
- TIBCO Project Mashling natively supports IoT communications protocols. For example, it was one of only two API gateways surveyed that natively supports Constrained Application Protocol (CoAP).

Weaknesses

- TIBCO Project Mashling has minimized its IAM features, relying on Mashery. This is a design choice to emphasize performance.
- Mashery administration functions are available only as a cloud service, which could be an issue for organizations looking for an entirely on-premises solution.
- None of the TIBCO gateway offerings support recent OIDC extensions.
- TIBCO Project Mashling lacks most of the security capabilities out of the box. This is largely a design choice to emphasize performance and flexibility for event-driven microservices. However, security capabilities can be extended through custom Go coding.

WSO2 API Manager, WSO2 API Cloud and WSO2 API Microgateway

WSO2 offers a full range of API gateway deployment options. WSO2 API Manager and WSO2 API Cloud are software and cloud service versions of the same code base. Some functions, such as support for MQTT and Advanced Message Queuing Protocol (AMQP), may be provided via WSO2 Enterprise Integrator (or via WebSockets). WSO2 provides additional IAM functionality via WSO2 Identity Server. For those gateway customers who need only the advanced key management part of

WSO2 Identity Server, there is a special IAM Key Manager server profile install that can directly replace the built-in Key Manager in WSO2 API Manager. Note that WSO2 API Manager 3.X, which has been rewritten to leverage WSO2's new Ballerina framework, was in prerelease as this research was written.

WSO2 provides feature parity in security capabilities across its on-premises, cloud service and microgateway offerings. It provides most of the security capabilities out of the box, with the exception of DDoS protection and specific bot mitigation functionality. However, malicious bot traffic aimed at APIs can be mitigated with WSO2's behavior-based stream processor. WSO2 provides some built-in rules and patterns to identify fraudulent and anomalous traffic. The rules are also customizable, and managed services can assist with such customizations. Some data security features, such as tokenization and encryption, also require custom plug-ins.

Strengths

- All of the WSO2 API gateway offerings are open source.
- The WSO2 gateways are stronger than average in their support for recent OAuth and OIDC extensions. They also offer robust STS functionality, and a RESTful STS capability is on the roadmap.
- WSO2 offers security feature parity across all deployment types. In most cases, the capabilities that WSO2 doesn't provide out of the box can be supplemented through custom code and rules.

Weaknesses

- Support for newer data storage formats, such as Microsoft Azure AD Graph API and GraphQL, requires customization.
- WSO2 does not provide DDoS protection natively or through partnership with another vendor. Organizations would need to select a separate vendor offering to mitigate risk of DDoS attacks against web APIs.
- WSO2 lacks security certifications for its products. However, compliance is less about having a certified gateway and more about properly deploying and configuring the gateway within a given application architecture. The gateway is used in regulated environments, such as those where Health Insurance Portability and Accountability Act (HIPAA) or Payment Card Industry Data Security Standard (PCI DSS) compliance must be satisfied.

The Details

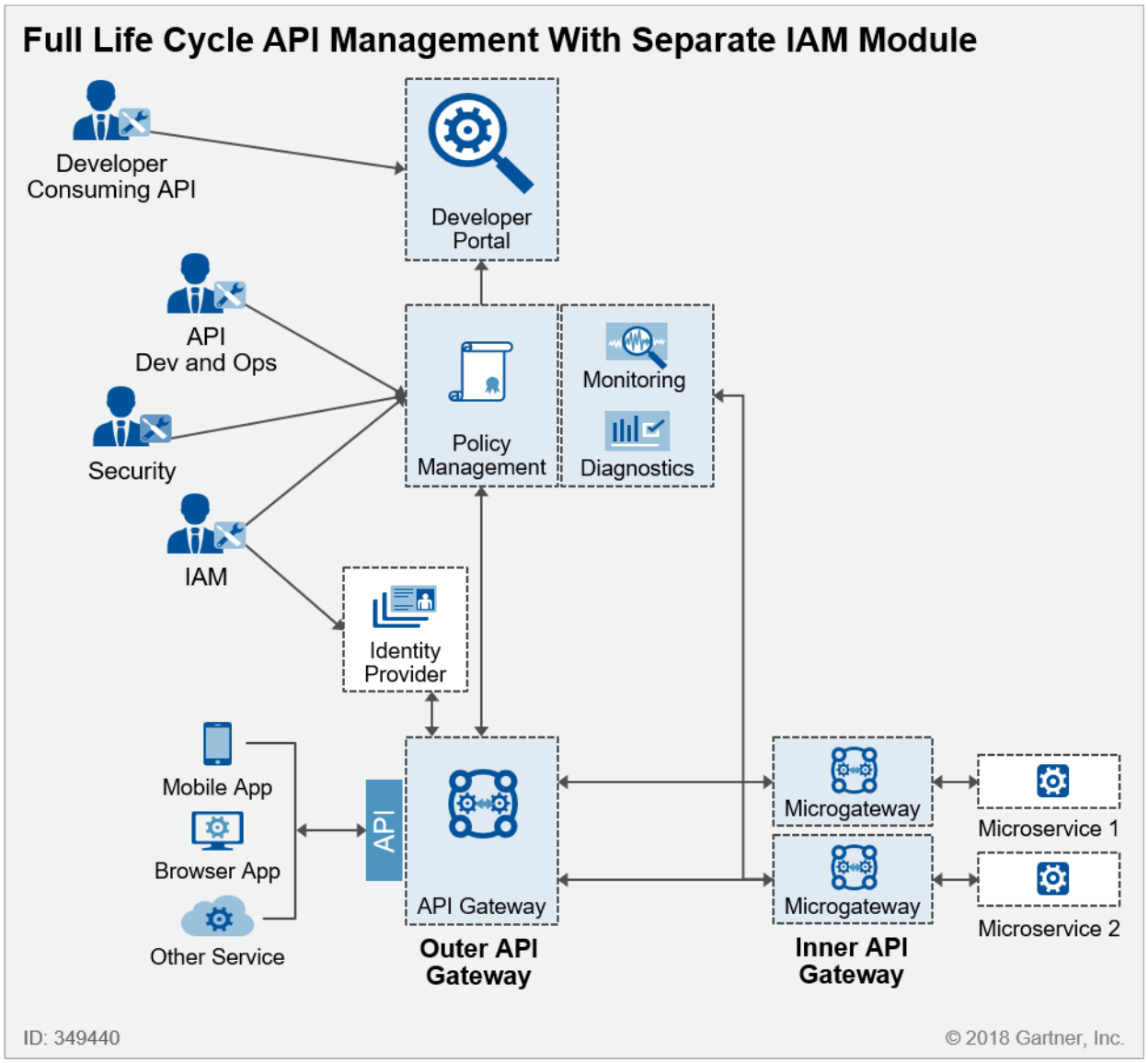
This document is a successor to "Selecting the Right API Gateway for Identity and Access Management." The document has been expanded to provide more detail on security and on high-level DevSecOps functions. The IAM features covered have evolved to include newer options (such as support for recent OAuth/OIDC extensions) and to eliminate some of the less relevant details. For example, support for particular social login identity providers has been dropped, but the ability to

adapt policy based on the identity provider has been added (see the IAM Score Details section below).

IAM Score Details

Identity and access management consists of a wide range of functions, and the specific IAM needs vary widely by use case. The IAM features evaluated here refer to a wide range of identity protocols. Some of these protocols are needed to support interaction with legacy infrastructure, while others are needed to support microservices architectures. As a best practice, most IAM functionality should be handled by the IAM system used to identify, authenticate and/or authorize the user, machine or API (see Figure 4).

Figure 4. Example of a Full Life Cycle API Management Deployment With a Separate IAM Module



Dev and Ops = development and operations

Source: Gartner (June 2018)

However, there is a wide range of IAM capabilities that some organizations are looking for in an API gateway or microgateway. For the purposes of this analysis, Gartner evaluated 40 IAM features, which are organized into seven groups. The first of these groups covers basic support for federation standards.

Identity Federation Standards

This section covers basic support for common identity federation standards. Figure 5 and Table 1 assess support for the following standards:

- **SAML IdP:** SAML identity provider (IdP). Note that, as a best practice, organizations should not use an IdP running on an API gateway in production.
- **SAML SP:** SAML service provider (SP), which can perform SAML token validation and de-encryption.
- **OAuth AS:** OAuth authorization server (AS). Note that most production deployments leverage an OAuth AS running on a separate IAM system (not on the API gateway.)
- **OAuth RS:** OAuth resource server (RS).
- **OIDC OP:** OIDC identity provider, referred to as an "OpenID provider" (OP).
- **OIDC RP:** OIDC resource provider (RP).

See also Figure 8 for more details about support for specific flows.

Figure 5. Part of IAM — Support for Identity Federation Standards

Part of IAM — Support for Identity Federation Standards

Offering	SAML IdP	SAML SP	OAuth AS	OAuth RS	OIDC OP	OIDC RP
Amazon API Gateway	3	3	3	4	3	4
Apigee Edge	4	4	4	4	4	4
Apigee Edge Microgateway	1	1	1	4	1	4
Axway API Gateway	2	2	4	4	4	4
CA Technologies API Gateway	4	4	4	4	4	4
CA Technologies Microgateway	1	1	3	4	1	1
IBM DataPower Gateway	4	4	4	4	4	4
IBM API Connect Microgateway	2	2	4	4	2	2
Kong Enterprise Edition	1	1	4	4	4	4
Microsoft Azure API Management	3	3	3	3	3	3
MuleSoft Mule	1	4	4	4	1	4
NGINX Plus	1	2	1	1	1	4
Red Hat 3scale APIcast API Gateway	4	4	4	4	4	4
Software AG webMethods API Gateway	3	4	4	4	4	4
TIBCO API Exchange Gateway	4	4	4	4	4	4
TIBCO Mashery Enterprise	1	4	4	4	2	4
TIBCO Project Mashling	1	1	1	1	1	1
WSO2 API Manager/API Cloud	4	4	4	4	4	4
WSO2 API Microgateway	4	4	4	4	4	4

Key:
Fill color correlates to the offering's strength in each listed criterion:
1 = None
2 = Via customization
3 = Via integration with another offering by the same vendor (all API gateways can integrate with other IAM systems via identity standards)
4 = Yes

ID: 349440

Source: Gartner (June 2018)

Table 1. Part of IAM — Support for Identity Federation Standards (Footnotes)

Offering	Notes
Amazon API Gateway	SAML IdP is supported via AWS SSO. SAML SP, OAuth AS and OIDC OP are supported via Amazon Cognito.
Apigee Edge	SAML SP requires custom code.
Axway API Gateway	SAML is supported via custom policies.
CA Technologies Microgateway	OAuth AS is supported via CA API Gateway.
IBM API Connect Microgateway	Support for SAML and OIDC is provided via Node.js modules.
Microsoft Azure API Management	Support is provided via Azure AD.
MuleSoft Mule	SAML and OAuth are supported via the Anypoint Platform. SAML IdP and OIDC OP are supported via third parties.
NGINX Plus	SAML SP is supported via custom code or third-party modules. OIDC RP is supported in R15 via plug-in.
Software AG webMethods API Gateway	SAML IdP can be used for development and testing purposes, but not for production via webMethods Integration Server. External IdPs can be configured within the product.
TIBCO Mashery Enterprise	TIBCO Mashery supports SAML, both as an IdP and as an SP, for SSO to its portal and administration applications. TIBCO Mashery does not support SAML for API authentication. OIDC OP requires customization.

Source: Gartner (June 2018)

OAuth Extensions

The OAuth 2.0 standard is continuing to evolve to meet new use cases and to improve security. Many of the newer extensions are not yet supported by all vendor offerings. Note that additional extensions are continuing to emerge. Figure 6 and Table 2 assess support for the following OAuth extensions:

- **Token Introspection:** This extension is defined in Internet Engineering Task Force (IETF) Request for Comments (RFC) 7662. It enables clients and resource servers to query an OAuth 2.0 AS to determine the active state of an OAuth 2.0 token and retrieve meta-information about that token. OAuth 2.0 deployments can use this method to convey information about the authorization context of the token, as an alternative, or complement, to using self-contained tokens (i.e., JSON Web Tokens [JWTs]).

- **JWT Signing Key Rotation and Discovery:** Publishing AS public signing keys enables resource servers and OIDC clients to discover currently used signing keys when validating JWTs.
- **Token Revocation:** As defined in IETF RFC 7009, the revocation endpoint enables clients to notify the AS that an access or refresh token is no longer needed.
- **Dynamic Client Registration:** Defined in IETF RFC 7591, this extension enables clients such as apps and microservices to dynamically register themselves at the authorization server.

Figure 6. Part of IAM — Support for OAuth Extensions

Part of IAM — Support for OAuth Extensions

Offering	Token Introspection	JWT Signing Key Rotation and Discovery	Token Revocation	Dynamic Client Registration
Amazon API Gateway	1	4	1	1
Apigee Edge	4	4	4	1
Apigee Edge Microgateway	1	4	1	1
Axway API Gateway	4	2	4	1
CA Technologies API Gateway	4	4	4	4
CA Technologies Microgateway	1	1	1	1
IBM DataPower Gateway	4	2	4	2
IBM API Connect Microgateway	1	1	1	1
Kong Enterprise Edition	4	4	4	4
Microsoft Azure API Management	2	4	2	1
MuleSoft Mule	4	2	2	4
NGINX Plus	1	2	1	1
Red Hat 3scale APIcast API Gateway	4	4	1	4
Software AG webMethods API Gateway	4	1	4	4
TIBCO API Exchange Gateway	4	1	4	4
TIBCO Mashery Enterprise	4	1	4	4
TIBCO Project Mashling	1	1	1	1
WSO2 API Manager/API Cloud	4	4	4	4
WSO2 API Microgateway	4	4	4	4

Key:
Fill color correlates to the offering's strength in each listed criterion:
1 = None
2 = Via customization
3 = Via integration with another offering by the same vendor (all API gateways can integrate with other IAM systems via identity standards)
4 = Yes

ID: 349440

Source: Gartner (June 2018)

Table 2. Part of IAM — Support for OAuth Extensions (Footnotes)

Offering	Notes
Apigee Edge	Apigee Edge supports JWT signing keys. When using algorithms like RSA, developers can implement key rotation (through the use of different KIDs) and discovery (through the use of JWKS).
Axway API Gateway	Basic token introspection is supported via the token information API. Anything else requires custom policy. JWT signing key rotation and discovery are supported via custom policy logic.
CA Technologies API Gateway	Support for token validation is provided via token validation endpoints exposed to resource servers. Support for discovery is provided OOTB, while support for JWT signing key rotation requires configuration. The gateway supports an OOTB custom flow that achieves a similar end result to RFC 7591 without 100% RFC support.
IBM DataPower Gateway	JWT signing key rotation, discovery and dynamic client registration are supported via custom code.
Microsoft Azure API Management	Support is provided via Azure AD. Token introspection and revocation are supported via integration policy.
MuleSoft Mule	JWT signing key rotation, discovery and token revocation are supported via customization.
NGINX Plus	JWT signing key rotation is supported via cron jobs.
KIDs = Key IDs; JWKS = JSON Web Key Set	

Source: Gartner (June 2018)

OIDC Extensions

The OIDC standard is also continuing to evolve to meet new use cases and to improve security. Many of the newer extensions are not yet supported by all vendor offerings. Note that additional extensions are continuing to emerge. Figure 7 and Table 3 assess support for the following OIDC extensions:

- **PKCE:** OAuth Proof Key for Code Exchange (PKCE; IETF RFC 7636). Designed for public clients that use the OAuth authorization code flow and have high-security needs, PKCE (pronounced "pixy") protects against authorization code interception attacks. It was published in August 2015. Many vendors still do not support this option, even though it's recommended for use with native clients, such as mobile apps, as part of the AppAuth pattern.
- **PoP:** OAuth proof of possession (PoP). PoP extends token security beyond bearer tokens. A PoP token flow ensures that a requesting client has possession of a cryptographic key known only by that client. By proving possession of the key in the PoP token, the client can assure a resource server that it's the intended owner of the PoP token. PoP tokens mitigate man-in-the-middle attacks and stolen tokens, and can bind a token to physical hardware. A presenter with

the ability to prove possession of a key is also sometimes described as a "holder of key." The specifications for how to prove possession of the keys has not been finalized as of this writing, but some vendors offer early implementations.

- **SAML and JWT Assertion Framework:** This extension provides a framework (IETF RFC 7521) for authorization servers to use SAML assertions (IETF RFC 7522) and JWTs (IETF RFC 7523) for client authentication and as grant types to request access tokens.
- **Discovery:** The ability to expose an OIDC discovery endpoint.
- **OIDC Request Parameter Prompt:** This feature is defined in the OpenID Connect Core 1.0 specification, but is not implemented by all vendors. This feature can enable an API gateway, when acting as an AS client, to perform step-up authentication.

Figure 7. Part of IAM — Support for OIDC Extensions

Part of IAM — Support for OIDC Extensions

Offering	PKCE	PoP	SAML and JWT Assertion Framework	Discovery	OIDC Request Parameter Prompt
Amazon API Gateway	3	1	3	1	1
Apigee Edge	4	2	4	4	1
Apigee Edge Microgateway	1	1	1	1	1
Axway API Gateway	2	2	4	1	1
CA Technologies API Gateway	4	1	4	4	4
CA Technologies Microgateway	1	1	1	1	1
IBM DataPower Gateway	4	4	4	2	1
IBM API Connect Microgateway	1	1	1	1	1
Kong Enterprise Edition	4	4*	1	4	4
Microsoft Azure API Management	3	3	3	3	3
MuleSoft Mule	1	1	1	1	1
NGINX Plus	1	1	1	1	1
Red Hat 3scale APIcast API Gateway	2	1	4	4	4
Software AG webMethods API Gateway	1	1	4	1	4
TIBCO API Exchange Gateway	1	1	1	1	1
TIBCO Mashery Enterprise	1	1	1	1	1
TIBCO Project Mashling	1	1	1	1	1
WSO2 API Manager/API Cloud	4	4*	4	3	3
WSO2 API Microgateway	4	4*	4	3	3

Key:
Fill color correlates to the offering's strength in each listed criterion:
1 = None
2 = Via customization
3 = Via integration with another offering by the same vendor (all API gateways can integrate with other IAM systems via identity standards)
4 = Yes

* Is on roadmap.
ID: 349440

Source: Gartner (June 2018)

Table 3. Part of IAM — Support for OIDC Extensions (Footnotes)

Offering	Notes
Amazon API Gateway	PKCE is supported via Amazon Cognito OIDC OPs. SAML and JWT assertion framework for OAuth 2.0 is supported via AWS STS and Amazon Cognito.
Apigee Edge	PKCE can be configured via the built-in OAuth, PopulateCache and LookupCache policies. The PoP token type could be supported via a Java callout that verifies the inbound token.
Axway API Gateway	PKCE and PoP are supported via custom policy logic.
CA Technologies API Gateway	PKCE is supported on the SDKs for both the CA API Gateway and the CA API Mobile Gateway. SAML and JWT assertion framework for OAuth 2.0 is supported for authorization grants only.
IBM DataPower Gateway	PoP uses mutual TLS. Assertion framework support is for JWT only (not SAML). Discovery is supported via custom code.
Kong Enterprise Edition	PoP is on the roadmap.
Microsoft Azure API Management	Support is provided via Azure AD
MuleSoft Mule	Extensions are supported only via third-party, OIDC-compliant authorization servers.
Red Hat 3scale APIcast API Gateway	PKCE is available as an optional extension.
Software AG webMethods API Gateway	Assertion framework support is for JWT only (not SAML).
WSO2 API Manager/API Cloud	PoP is on the roadmap. Support for discovery and OIDC Request Parameter Prompt requires the integration of WSO2 Identity Server, or the IAM Key Manager server profile.
WSO2 API Microgateway	PoP is on the roadmap. Support for discovery and OIDC Request Parameter Prompt requires the integration of WSO2 Identity Server, or the IAM Key Manager server profile.

SDKs = software development kits; TLS = Transport Layer Security

Source: Gartner (June 2018)

OAuth/OIDC Flows

As use cases continue to expand, newer OAuth and OIDC flows continue to be added. Vendors generally support the more standard flows, but often lag in their support for newer flows. Figure 8 and Table 4 assess support for the following flows:

- **OAuth Authorization Code:** This flow supports refresh tokens. Note that it is not appropriate for use with public clients unless used in conjunction with PKCE.

- **OAuth Client Credentials:** This flow is suitable for service-to-service API calls.
- **OAuth Implicit:** This flow does not support refresh tokens and is suitable for use with browser-based apps.
- **OAuth Resource Owner Password Credentials:** This flow is suitable for trusted situations where the resource owner provides the client with its username and password. It supports refresh tokens.
- **OAuth Device:** This flow is suitable for browserless and input-constrained "faceless" devices that do not provide any input capabilities.
- **OIDC Authorization Code:** This flow supports refresh tokens.
- **OIDC Hybrid:** This flow is a hybrid of the authorization code and implicit flows (see below). Tokens can be delivered by both the authorization and the token endpoints. This is the flow supported by the Azure AD OpenID provider.
- **OIDC Implicit:** This flow does not support refresh tokens and is suitable for use with browser-based apps.

Figure 8. Part of IAM — Support for OAuth/OIDC Flows

Part of IAM — Support for OAuth/OIDC Flows

	OAuth					OIDC		
Offering	Authorization Code	Client Credentials	Implicit	Resource Owner Password Credentials	Device	Authorization Code	Hybrid	Implicit
Amazon API Gateway	3	3	3	1	1	3	1	3
Apigee Edge	4	4	4	4	2	4	4	4
Apigee Edge Microgateway	4	4	4	4	1	1	1	1
Axway API Gateway	4	4	4	4	1	4	4	4
CA Technologies API Gateway	4	4	4	4	2	4	4	4
CA Technologies Microgateway	1	1	1	1	1	1	1	1
IBM DataPower Gateway	4	4	4	4	2	4	4	4
IBM API Connect Microgateway	4	4	4	4	1	2	2	2
Kong Enterprise Edition	4	4	4	4	4	4	4	4
Microsoft Azure API Management	4	4	4	4	1	4	4	4
MuleSoft Mule	4	4	4	4	4	1	1	1
NGINX Plus	1	1	1	1	1	4	1	4
Red Hat 3scale APIcast API Gateway	4	4	4	4	1	4	4	4
Software AG webMethods API Gateway	4	4	4	1	1	4	1	4
TIBCO API Exchange Gateway	4	4	1	4	1	4	1	1
TIBCO Mashery Enterprise	4	4	4	4	1	1	1	1
TIBCO Project Mashling	1	1	1	1	1	1	1	1
WSO2 API Manager/API Cloud	4	4	4	4	2	4	4*	4
WSO2 API Microgateway	4	4	4	4	2	4	4*	4

Key:
Fill color correlates to the offering's strength in each listed criterion:
1 = None
2 = Via customization
3 = Via integration with another offering by the same vendor (all API gateways can integrate with other IAM systems via identity standards)
4 = Yes
* Is on roadmap.

ID: 349440

Source: Gartner (June 2018)

Table 4. Part of IAM — Support for OAuth/OIDC Flows (Footnotes)

Offering	Notes
Amazon API Gateway	Amazon API Gateway supports the following flows via Amazon Cognito: ■ OAuth authorization code, client credentials and implicit ■ OIDC authorization code and implicit
Apigee Edge	The OAuth device flow is not natively supported by Apigee Edge. However, it could be supported via a configuration relying on the following: ■ The Apigee Edge cache ■ A nonce that can be generated and transmitted to the device, and then later verified by user interaction
CA Technologies API Gateway	Support for the OAuth device flow is via policy configuration.
IBM DataPower Gateway	Support for the OAuth device flow is via custom code.
IBM API Connect Microgateway	Support for OIDC flows can be created via JavaScript code, along with Node.js modules from the open-source community.
MuleSoft Mule	OAuth is supported via the Anypoint Enterprise Security OAuth 2.0 provider, which enables the OAuth flows. OIDC OPs and, therefore, OIDC flows are supported only via third parties
NGINX Plus	The OIDC authorization code flow is supported in NGINX Plus R15.
WSO2 API Manager/API Cloud	Support for the OAuth device flow is available via extensions. Support for the OIDC hybrid flow is on the roadmap.
WSO2 API Microgateway	Support for the OAuth device flow is available via extensions. Support for the OIDC hybrid flow is on the roadmap.

Source: Gartner (June 2018)

Identity Token Transformation

Most established organizations use multiple token types and formats to access various systems. Thus, they need the ability to translate (or transform) token types from one format to another. This translation capability is performed by a security token service. Note that not all organizations need support for all of these formats. The translation function may be performed on an IAM system or on an API gateway. Figure 9 and Table 5 assess support for the following formats:

- **Kerberos Ticket:** Kerberos is an integral part of the security system in Microsoft Active Directory. Support for this format is generally needed only in gateways that directly contact Microsoft AD and that interface with legacy systems. Thus, such support is typically not necessary in microgateways. It is more common for an STS to be able to accept a Kerberos

ticket as an input format. The ability to generate one as an output is a plus for some organizations.

- **SAML Token:** SAML is commonly used as both an input and an output format, especially for accessing SaaS and legacy, browser-based applications.
- **JWT:** A JWT is a signed and possibly encrypted token format used by OIDC and, sometimes, by OAuth 2.0. JWT is commonly used as both an input and an output format.
- **X.509 Certificate:** X.509 is a credential issued from a public-key infrastructure (PKI). It's used to secure service-to-service communications. A full-featured gateway should be able to accept an X.509 certificate as an authentication method.
- **OAuth Bearer Token:** This is a token format used by OIDC and OAuth 2.0.
- **Cookie:** Cookies have proprietary formats. They're also known as web access management (WAM) tokens or session cookies. Examples include those used by CA Single Sign-On, Entrust GetAccess, ForgeRock's Access Management (formerly OpenAM), IBM Security Access Manager, Oracle Access Management Access Manager, Micro Focus (NetIQ) and Ping Identity's PingFederate Server. Support for this format was traditionally needed in gateways that interface with legacy systems. Cookies can also be used in conjunction with OAuth to extend SSO across associated, native applications. WAM is also used to support single-page applications (SPAs). As noted in Table 5, a few of the API gateway vendors not only support token transformation to proprietary cookie formats, but also provide native support for agent or proxy-based WAM. Note that a newer, more-standards-based approach to WAM is to use OIDC. However, many organizations still need to interoperate with systems that use proprietary cookies rather than JWTs.
- **REST-Based STS:** Traditional STS implementations did not support REST-based interfaces. Modern deployment architectures can benefit from an STS that supports REST-based interfaces, either through proprietary means or by using the IETF OAuth 2.0 Token Exchange specification draft. The IETF draft defines how authorization servers can expose an STS endpoint for clients to request tokens. It also includes functionality for delegation and impersonation of identities.

Figure 9. Part of IAM — Support for Identity Token Transformation

Part of IAM — Support for Identity Token Transformation

	Kerberos Ticket	SAML Token	JWT	X.509 Certificate	OAuth Bearer Token	Cookie	REST-Based STS
Amazon API Gateway	3	3	3	1	3	1	1
Apigee Edge	4	4	4	4	4	4	4
Apigee Edge Microgateway	1	1	3	1	3	1	1
Axway API Gateway	4	4	4	4	4	4	2
CA Technologies API Gateway	4	4	4	4	4	2	4
CA Technologies Microgateway	1	1	3	1	1	1	1
IBM DataPower Gateway	4	4	4	4	4	4	1
IBM API Connect Microgateway	2	2	2	2	1	1	1
Kong Enterprise Edition	2	4*	4	4	4	1	4
Microsoft Azure API Management	3	4	4	4	4	1	3
MuleSoft Mule	4	2	2	4	4	2	4
NGINX Plus	1	1	4	2	1	2	2
Red Hat 3scale APIcast API Gateway	1	4	4	4	4	2	1
Software AG webMethods API Gateway	4	4	4	4	4	2	1
TIBCO API Exchange Gateway	4	4	2	1	4	2	4
TIBCO Mashery Enterprise	1	1	2	1	4	2	4
TIBCO Project Mashling	2	2	2	2	2	2	2
WSO2 API Manager/API Cloud	3	3	3	3	3	2	3*
WSO2 API Microgateway	3	3	3	3	3	2	3*

Key:
Fill color correlates to the offering's strength in each listed criterion:
1 = None
2 = Via customization
3 = Via integration with another offering by the same vendor (all API gateways can integrate with other IAM systems via identity standards)
4 = Yes

* Is on roadmap.

ID: 349440

Source: Gartner (June 2018)

Table 5. Part of IAM — Support for Identity Token Transformation (Footnotes)

Offering	Notes
Amazon API Gateway	Support for STS functionality is provided via AWS STS and Amazon Cognito. Customers can translate a Kerberos ticket to a SAML assertion via AWS STS. Support for JWT is provided via the AWS IAM AssumeRoleWithWebIdentity API or through integration with Amazon Cognito. Support for OAuth access tokens is provided via Amazon Cognito.
Apigee Edge Microgateway	The microgateway uses Apigee Edge.
Axway API Gateway	The gateway's STS supports CA, IBM, Oracle and NetIQ session cookies. The gateway includes native support for proxy-based WAM. The STS is proxy-session-based. It can expose REST APIs to perform token exchange via custom policies.
CA Technologies API Gateway	Support for CA session cookies is provided OOTB. For other proprietary cookie support, the STS can extract a token from session information if present in a message context. It can also use policy to construct a token in whatever format is required. The gateway includes native support for proxy-based WAM. It can be configured to interface with agent-based WAM. The STS can be configured to support various interaction methods, including stand-alone WS-Trust and REST-based token exchange. It can also be configured as a proxy for token mediation.
IBM DataPower Gateway	Support for CA and IBM session cookies is provided OOTB. Support for Oracle, NetIQ and PingIdentity session cookies requires custom code. Support for proxy-based WAM is provided via built-in integration with IBM Security Access Manager and CA Single Single-On.
IBM API Connect Microgateway	Kerberos tickets, SAML tokens, JWTs and X.509 certificates are supported via Node.js modules.
Kong Enterprise Edition	Support for SAML tokens is on the roadmap. Kerberos tickets are supported via plug-in. Kong also supports HMAC and LDAP. It includes native support for proxy-based WAM.
Microsoft Azure API Management	Kerberos tickets are supported via Azure AD Application Proxy. RESTful STS is supported via Azure AD.
MuleSoft Mule	SAML tokens and JWTs are supported via custom policies. Cookie support covers only PingIdentity session cookies.
NGINX Plus	All JWT claims and X.509 certificate attributes are available as configuration variables (and to Lua/JavaScript extensions) that can be used to decorate upstream requests with identity information. Support for CA Single Sign-On, ForgeRock, Keycloak, Okta and PingIdentity cookies is available by plug-in. Auth_request_module allows authentication configuration via a REST service.
Red Hat 3scale APIcast API Gateway	Proprietary cookie support is possible with customization. The gateway includes native support for both proxy- and agent-based WAM.
Software AG webMethods API Gateway	Support for CA, IBM and Oracle session cookies is possible with customization.
TIBCO API Exchange Gateway	Support for JWTs or cookies requires customization.

Offering	Notes
TIBCO Project Mashling	STS functionality can be customized.
WSO2 API Manager/API Cloud	Support for token transformation requires integration of WSO2 Identity Server, or the IAM Key Manager server profile. Support for cookies is available via extension. WSO2 can also transform tokens between SAML, OIDC, CAS and WS-Federation. Support for Token Exchange RFC (RESTful STS) is on the roadmap.
WSO2 API Microgateway	Support for token transformation requires integration of WSO2 Identity Server, or the IAM Key Manager server profile. Support for cookies is available via extensions. Support for proxy- and agent-based WAM is also available via extensions. Support for Token Exchange RFC (RESTful STS) is on the roadmap.
CAS = Central Authentication Service; HMAC = hash-based message authentication code	

Source: Gartner (June 2018)

Directly Connected User Data Stores

Figure 10 and Table 6 assess support for the following formats:

- **LDAP:** Lightweight Directory Access Protocol, which is commonly used for both employee and customer data stores.
- **Microsoft AD:** Microsoft Active Directory.
- **JDBC:** Java Database Connectivity.
- **Microsoft Azure AD Graph API:** Microsoft Azure AD user data can be accessed via the Azure Active Directory Graph API.
- **GraphQL:** GraphQL has emerged as an alternative to RESTful interfaces. GraphQL allows client implementations to define a specific structure for data returned from the server. This provides the benefit of retrieving only exactly what the client needs.

Figure 10. Part of IAM — Support for Directly Connected User Data Stores

Part of IAM — Support for Directly Connected User Data Stores

	LDAP	Microsoft AD	JDBC	Microsoft Azure AD Graph API	GraphQL
Amazon API Gateway	2	2	2	2	2
Apigee Edge	4	4	4	4	4
Apigee Edge Microgateway	3	3	3	3	3
Axway API Gateway	4	4	4	1	1
CA Technologies API Gateway	4	4	4	1	1
CA Technologies Microgateway	4	4	4	1	1
IBM DataPower Gateway	4	4	4	2	2
IBM API Connect Microgateway	4	2	1	1	1
Kong Enterprise Edition	4	2	1	4*	4
Microsoft Azure API Management	2	4	2	4	2
MuleSoft Mule	4	4	4	1	4
NGINX Plus	4	2	1	2	1
Red Hat 3scale APIcast API Gateway	4	4	4	4	4
Software AG webMethods API Gateway	4	2	4	1	1
TIBCO API Exchange Gateway	4	4	2	2	2
TIBCO Mashery Enterprise	4	4	2	2	2
TIBCO Project Mashling	1	1	1	1	1
WSO2 API Manager/API Cloud	4	4	4	2	2
WSO2 API Microgateway	4	4	4	2	2

Key:
Fill color correlates to the offering's strength in each listed criterion:
1 = None
2 = Via customization
3 = Via integration with another offering by the same vendor (all API gateways can integrate with other IAM systems via identity standards)
4 = Yes

* Is on roadmap.
ID: 349440

Source: Gartner (June 2018)

Table 6. Part of IAM — Support for Directly Connected User Data Stores

Offering	Notes
Amazon API Gateway	Data stores are supported via custom authorizers.
CA Technologies API Gateway	Other supported formats include: ■ Apache Cassandra (OOTB) ■ Apache MongoDB (upon request) ■ SCIM 2.0 for managing identities (requires customization)
CA Technologies Microgateway	MongoDB is also supported (upon request).
IBM API Connect Microgateway	Microsoft AD integration is supported via Node.js modules.
Kong Enterprise Edition	Microsoft AD is supported via OIDC. Support for Microsoft Azure AD Graph API is on the roadmap. Kong EE can proxy GraphQL, as long as the data is just plain JSON.
Microsoft Azure API Management	JDBC support requires Azure AD. LDAP, JDBC and GraphQL are supported via integration policy.
NGINX Plus	Microsoft AD and Azure AD are supported via OIDC.
Software AG webMethods API gateway	Microsoft AD is supported via LDAP.
WSO2 API Manager/API Cloud	Microsoft Azure AD Graph API and GraphQL are supported via extensions. SCIM 1.1 and 2.0 are also supported.

SCIM = System for Cross-Domain Identity Management

Source: Gartner (June 2018)

Adaptive, Context-Based Authentication

Adaptive, context-based access refers to the ability to vary access policy logic by specified access attributes. Many vendors are able to leverage any available attribute in their access policy logic. For example, some vendors can vary access policy:

- **By Identity Provider:** The ability to vary access policy by the identity provider (e.g., an internal SAML provider versus a social identity provider).
- **By IP Address:** The ability to vary access policy by Internet Protocol (IP) address or IP address range.
- **By License:** The ability to vary access policy depending on how the API is licensed.
- **By API Key:** The ability to vary access policy by API key. Note that Gartner recommends using OAuth 2.0 rather than API keys to protect access to APIs.

- **By Digital Signature Verification:** The ability to vary access policy according to the presence of a digital signature.

Figure 11 and Table 7 assess support for options above.

Figure 11. Part of IAM — Support for Adaptive, Context-Based Authentication

Part of IAM — Support for Adaptive, Context-Based Authentication

	By Identity Provider	By IP Address	By License	By API Key	By Digital Signature Verification
Amazon API Gateway	3	3	2	2	2
Apigee Edge	4	4	4	4	4
Apigee Edge Microgateway	4	4	4	4	4
Axway API Gateway	4	4	1	4	4
CA Technologies API Gateway	4	4	4	4	4
CA Technologies Microgateway	4	4	4	4	4
IBM DataPower Gateway	4	4	4	4	4
IBM API Connect Microgateway	2	4	1	4	2
Kong Enterprise Edition	4	4	4	4	4
Microsoft Azure API Management	4	4	4	4	4
MuleSoft Mule	2	4	2	4	2
NGINX Plus	4	4	1	4	4
Red Hat 3scale APIcast API Gateway	1	1	1	1	1
Software AG webMethods API Gateway	4	4	1	4	4
TIBCO API Exchange Gateway	2	2	1	4	4
TIBCO Mashery Enterprise	2	2	1	2	2
TIBCO Project Mashling	2	1	1	1	1
WSO2 API Manager/ API Cloud	4	2	2	4	2
WSO2 API Microgateway	4	2	2	4	2

Key:
Fill color correlates to the offering's strength in each listed criterion:
1 = None
2 = Via customization
3 = Via integration with another offering by the same vendor (all API gateways can integrate with other IAM systems via identity standards)
4 = Yes

ID: 349440

Source: Gartner (June 2018)

Table 7. Part of IAM — Support for Adaptive, Context-Based Authentication Footnotes

Offering	Notes
Amazon API Gateway	Context-based authentication by IdP or IP address is supported via AWS IAM. All of the context elements in Figure 11 can be included as part of the context provided to the Lambda authorizer REQUEST configuration.
Apigee Edge	Support for digital signatures is implicit with JWT. Some customers use HMAC based on the content or headers of the payload. Others use HTTPSignature.
Apigee Edge Microgateway	Support for digital signatures is implicit with JWT verification. Because the microgateway is built on Node.js, extension of the microgateway to verify digital signatures using other formats (like HMAC, HTTPSignature and Hawk) is straightforward.
Microsoft Azure API Management	Context-based authentication configured by license may also be configured by product, which is a group of one or more APIs that are licensed together.
MuleSoft Mule	Context-based authentication by IdP, license and digital signature is supported via custom policy.
NGINX Plus	Digital signature verification is based on X.509 client certificate attributes.
TIBCO API Exchange Gateway	The TIBCO API Exchange Gateway supports context-based authentication by either API keys or digital signatures OOTB. With the provided development tools, it is possible to fully customize and extend the authentication and validation options. Customers can do this by themselves, or they can work with the TIBCO Professional Services Group.
TIBCO Mashery Enterprise	Content-based authentication by IP address is supported via custom adapters. Customers can develop these adapters using the TIBCO Adapter SDK. Once developed, these adapters can be configured via the TIBCO Mashery API Control Center by the customer administrator.
WSO2 API Manager/API Cloud	Context-based authentication by IP address, license and digital signature verification is supported via extension.

Source: Gartner (June 2018)

Security Score Details

In some organizations, the practical application of "security" within an API context is often limited to controls such as transport encryption, access control, rate limiting and IP address blacklisting. This varies slightly from the application security practitioner space, where security is expanded to include DoS/DDoS protection, exploit mitigation and abuse mitigation. Vendors sometimes create confusion by using the more nebulous definition of "security" for their products. Therefore, it is important to distinguish the security features. This is especially true if you are relying on the API gateway as the sole enforcer of security controls. Some aspects of API management and API gateways are also tangentially beneficial for security. Examples include schema validation, schema export (for use in other tools) and API catalog.

Most of the vendors support more advanced security capabilities via customization or via integration with other application-layer components. An API gateway can be paired relatively easily with some other application-layer device, or with a cloud service, to offer a full range of security capabilities as part of a larger application infrastructure. However, this approach can start to introduce additional complexity, potential failure points and latency in a system design. This topic is covered in the research "Protecting Web Applications and APIs From Exploits and Abuse."

The security capabilities of the API gateway vendors were measured across three major categories:

- Traffic management
- Content inspection and threat protection
- Data security

For the purposes of this analysis, the security features evaluated are organized into three figures, one for each subcategory.

Product focus areas for vendors are not mutually exclusive but can be competing at times, especially in the microgateway variant, where performance is the primary concern. The three main reasons cited were:

1. Microgateways are used to manage dependencies/routing between interservice traffic in microservices architecture or mesh app and service architecture (MASA). Therefore, these inner gateways have less need for some types of protections, as these protections have already been implemented closer to the edge.
2. Buyers don't seek security capabilities and the traditional functionality of an API gateway in one component. There are often separate teams implementing and operating the gateways within the organization.
3. Extensive content inspection and analysis of API traffic slow performance. This is especially true with microgateways, which are performance-oriented and designed to be part of microservices architectures. Single-digit millisecond latency may be too slow, and high security becomes a nonstarter. Sidecar proxy deployments and nonblocking functionality are growing trends among vendors.

Vendors may state support for a given security or IAM capability by building custom code, which is a less-than-ideal method of delivery. It can potentially lead to misconfiguration or security gaps for the organization implementing the product. Custom code, in the case of the microgateway, is often Node.js or JavaScript. Neglecting to address security in custom code can result in critical weaknesses in an overall application design. The same holds true for improperly implementing a component, such as an identity protocol, data encryption or key management.

Application teams should import well-vetted Node.js and JavaScript security dependencies. In the worst case, security functions and protections are created from scratch and are ineffective. Vetting of dependencies and validation of custom code are necessary in these custom-code scenarios. This topic is covered in the research "How to Integrate Application Security Testing Into a Software Development Life Cycle."

Traffic Management

Traffic management capabilities control the ways a published API can be consumed. They are useful for controlling how much a machine or user can call an API, as well as for determining whether the caller is permitted at all.

Figure 12 assesses support for the following the traffic management capabilities:

- **Rate or Use Limiting:** The ability to control how frequently a caller can request data or functionality from an API. Limiting may be based on data rate, quotas for a given API consumer, acceptable use within a given time window or other usage patterns. It may also be referred to as "throttling."
- **DDoS Protection:** The ability to mitigate DDoS attacks, especially volumetric attacks. DDoS attacks can be problematic for external APIs and are more difficult to mitigate. Protection requires the use of cloud-based services and cloud scrubbing centers. Denial-of-service mitigation is included for most of the vendors, and it is often accomplished through a combination of other traffic management functions. IP address blacklisting and rate limiting can be effective for mitigation, but these techniques may not scale well in large deployments if the blacklists are static.
- **IP Address Blacklisting:** The ability to block a given IP address or range of IP addresses from consuming a given API.
- **IP Address Whitelisting:** The ability to explicitly allow a given IP address or range of IP addresses to consume a given API. Whitelisting is useful in more complex application infrastructures, where the organization may not want other integrated services to be subject to traffic management controls.

Figure 12. Part of Security — Traffic Management Support

Part of Security — Traffic Management Support

Offering	Rate or Use Limiting	DDoS Protection	IP Address Blacklisting	IP Address Whitelisting
Amazon API Gateway	4	3	4	4
Apigee Edge	4	4	4	4
Apigee Edge Microgateway	4	4	4	4
Axway API Gateway	4	1	4	4
CA Technologies API Gateway	4	1	4	4
CA Technologies Microgateway	4	1	4	4
IBM DataPower Gateway	4	3	2	2
IBM API Connect Microgateway	1	1	2	2
Kong Enterprise Edition	4	1	4	4
Microsoft Azure API Management	4	3	4	4
MuleSoft Mule	4	4	4	4
NGINX Plus	4	3	4	4
Red Hat 3scale APIcast API Gateway	4	1	4	4
Software AG webMethods API Gateway	4	1	4	4
TIBCO API Exchange Gateway	4	1	4	4
TIBCO Mashery Enterprise	4	4	4	4
TIBCO Project Mashling	2	1	2	2
WSO2 API Manager/API Cloud	4	1	4	4
WSO2 API Microgateway	4	1	4	4

Key:
Fill color correlates to the offering's strength in each listed criterion:
1 = None
2 = Via customization
3 = Via integration with any other product
4 = Yes
ID: 349440

Source: Gartner (June 2018)

Content Inspection and Threat Protection

Many API gateway vendors state support for exploit mitigation, but it's often accomplished through content inspection policies. Content inspection requires manual configuration of XML or JSON policies. These policies enforce API schema (a type of whitelisting) or regular expression (regex) blacklists to identify known malicious attacks, such as XSS or SQL injection patterns.

As offered by API gateway vendors, this type of exploit mitigation doesn't typically include the application profiling seen with some of the WAF vendors. In addition, content inspection policies

may be limited to defining acceptable parameters for API requests, as opposed to defining explicit patterns that might be used in injection attacks. Such parameters may include variable length, number of objects and payload size.

Vendors may also provide capability to define custom message handlers to analyze and manipulate traffic as needed for exploit mitigation. Others integrate with dedicated security controls like WAFs to do the heavy lifting of exploit mitigation. This integration may be accomplished through modules, plug-ins or extensions in the API gateway in order to avoid implementing another in-line device in the API traffic flow.

Figure 13 assesses support for the following content inspection and threat protection features:

- **Exploit Mitigation:** This feature detects and blocks API requests that are attempting to exploit vulnerabilities within the API or within the integrated application that the API communicates with. Such attacks commonly involve techniques like SQL injection, XML injection and cross-site scripting (XSS).
- **Bot Mitigation:** This feature detects and blocks API requests attempting to abuse API functionality. These requests typically originate from automated threats such as bots or botnets, and they are different from exploit cases. Abuse is more specific to business functionality provided by the API. Some common abuse cases include brute-forcing, scraping, aggregating, scalping and spamming.
- **Behavior Analysis:** This feature analyzes API traffic for behaviors that are malicious, anomalous or undesirable. Behavior analysis can be useful for uncovering exploits, abuses or other events, such as fraud.

Some of the vendors rely on behavior analysis to detect potential abuse and malicious bot behavior. This can be leveraged as a form of bot detection, but it is not a replacement for specific bot mitigation functionality. Moreover, bot mitigation for all vendors is not as advanced as the functionality you will find with dedicated bot mitigation solutions, such as those offered by Distil Networks, PerimeterX, Shape Security, ShieldSquare or Stealth Security.

Figure 13. Part of Security — Content Inspection and Threat Protection Support

Part of Security — Content Inspection/Threat Protection Support

Offering	Exploit Mitigation	Bot Mitigation	Behavior Analysis
Amazon API Gateway	3	1	3
Apigee Edge	4	3	3
Apigee Edge Microgateway	4	1	3
Axway API Gateway	2	1	1
CA Technologies API Gateway	4	1	4
CA Technologies Microgateway	4	1	4
IBM DataPower Gateway	4	3	3
IBM API Connect Microgateway	1	1	1
Kong Enterprise Edition	3	3	3
Microsoft Azure API Management	3	1	1
MuleSoft Mule	4*	1	4
NGINX Plus	3	3	1
Red Hat 3scale APIcast API Gateway	3	3	3
Software AG webMethods API Gateway	4	1	3
TIBCO API Exchange Gateway	4	1	1
TIBCO Mashery Enterprise	2	1	1
TIBCO Project Mashling	2	1	1
WSO2 API Manager/API Cloud	4	4	4
WSO2 API Microgateway	4	4	4

Key:
Fill color correlates to the offering's strength in each listed criterion:
1 = None
2 = Via customization
3 = Via integration with any other product
4 = Yes
* Is on roadmap.
ID: 349440

Source: Gartner (June 2018)

Data Security

Data security capabilities are those features that go above and beyond enforcement of transport encryption with TLS to protect data in transit.

Figure 14 assesses support for the following data security functions, which provide additional capability to act on, or transform, data within API payloads:

- **Block Message With Sensitive Data:** This function detects sensitive data, such as personally identifiable information (PII) and personal health information (PHI), and drops the API traffic.
- **Data Masking:** This function masks data within an API payload, typically via character substitution based on customizable patterns (e.g., replacing cardholder account numbers with the "*" character).
- **Data Tokenization:** This function tokenizes data within an API payload by replacing a specific value with a substitute value or token that can be retrieved later using a value-token mapping or other reversible algorithm.
- **Data Encryption:** This function encrypts or hashes data within an API payload by replacing a specific plain-text value with an encrypted or hashed alternate. Techniques include one-way hashing, symmetric encryption or asymmetric encryption.

Data masking, tokenization and encryption are covered further in the research "Protecting PII and PHI With Data Masking, Format-Preserving Encryption and Tokenization."

Figure 14. Part of Security — Data Security Support

Part of Security — Data Security Support

Offering	Block Message With Sensitive Data	Data Masking	Data Tokenization	Data Encryption
Amazon API Gateway	1	1	2	3
Apigee Edge	4	4	3	4
Apigee Edge Microgateway	2	2	2	2
Axway API Gateway	4	4	2	4
CA Technologies API Gateway	4	4	4	4
CA Technologies Microgateway	4	4	4	1
IBM DataPower Gateway	4	4	3	4
IBM API Connect Microgateway	1	2	2	1
Kong Enterprise Edition	2	2	2	2
Microsoft Azure API Management	4	4	1	4
MuleSoft Mule	4	4	4	4
NGINX Plus	2	2	1	1
Red Hat 3scale APIcast API Gateway	4	3	3	4
Software AG webMethods API Gateway	4*	4*	3	3
TIBCO API Exchange Gateway	4	4	1	4
TIBCO Mashery Enterprise	4	2	1	1
TIBCO Project Mashling	2	2	2	2
WSO2 API Manager/API Cloud	4	2	2	2
WSO2 API Microgateway	4	2	2	2

Key:
Fill color correlates to the offering's strength in each listed criterion:
1 = None
2 = Via customization
3 = Via integration with any other product
4 = Yes
* Is on roadmap.
ID: 349440

Source: Gartner (June 2018)

Evolving API Security Offerings

There is an evolving and sometimes-overlapping category of "API security" vendors and products that are focused on protecting web APIs. You can provide security and protection of web APIs with the combination of IAM, API gateways, WAFs and bot mitigation, as part of a larger enterprise architecture. These dedicated "API security" solutions exist as a variation of API management and, ultimately, still rely on an API gateway (or microgateway) as a proxy to enforce policies. They are not

designed to replace traditional API management and API gateways. Rather, they are designed to complement those tools. Some of these vendor products — two of which appear in this comparison through integrations or partnerships — include 42Crunch, Apigee Sense, Cloudentity Security Mesh, Ping Identity PingIntelligence for APIs (formerly Elastic Beam) and Salt (formerly Secful).

The product space is still evolving, but some common criteria that these tools or platforms exhibit include:

- An emphasis on the cloud service delivery model
- An API management interface focused on access control and on the security criteria defined in this analysis (traffic management, content inspection and threat protection, and data security)
- An edge API gateway, API microgateway, sidecar proxy or API plug-in to enforce policies
- API traffic security monitoring that leverages some combination of behavior analysis, threat analytics and threat intelligence
- A developer self-service portal for enabling protections and monitoring APIs
- Other functionality specific to microservices architectures and service meshes, such as:
  - Access control and microsegmentation for workloads
  - Workload attestation and mutual TLS to secure communications between workloads within the service mesh

DevSecOps Enablement Score Details

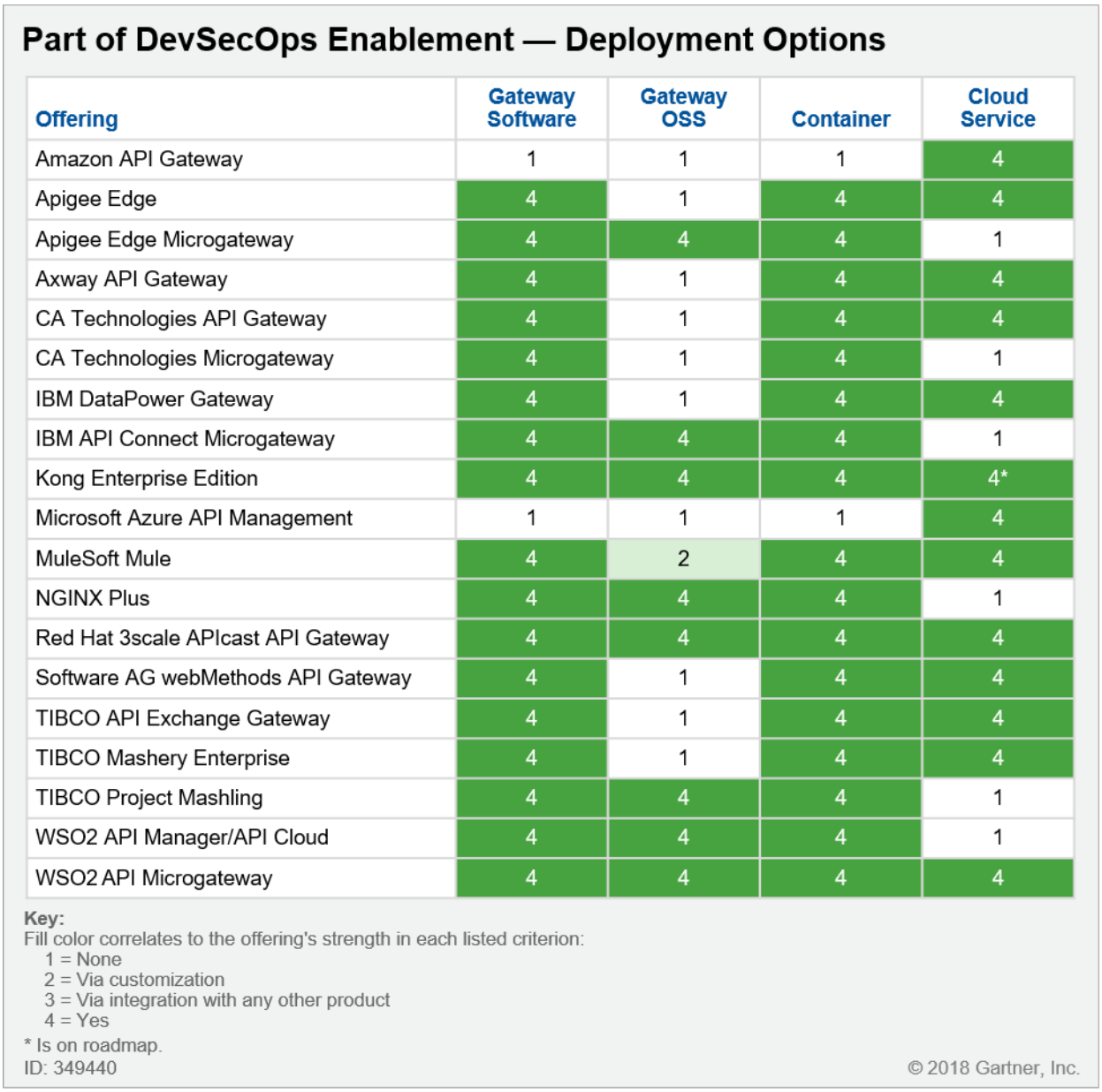
Protecting APIs and microservices requires development, security and operations (DevSecOps) flexibility. To fully automate and orchestrate the complete API life cycle, organizations must also automate and orchestrate security and protection considerations. An organization's gateways need to support flexible deployment options and operations automation. For the purposes of this analysis, the DevSecOps enablement features evaluated are organized into two figures. Note that a complete treatment of DevOps is outside the scope of this research.

Deployment Options

Figure 15 and Table 8 assess support for the following core deployment options:

- **Gateway Software:** The gateway is offered as software.
- **Gateway OSS:** The gateway software is open source.
- **Container:** The gateway software is containerized.
- **Cloud Service:** The gateway is offered as a cloud service.

Figure 15. Part of DevSecOps Enablement — Deployment Options



Part of DevSecOps Enablement — Deployment Options

Offering	Gateway Software	Gateway OSS	Container	Cloud Service
Amazon API Gateway	1	1	1	4
Apigee Edge	4	1	4	4
Apigee Edge Microgateway	4	4	4	1
Axway API Gateway	4	1	4	4
CA Technologies API Gateway	4	1	4	4
CA Technologies Microgateway	4	1	4	1
IBM DataPower Gateway	4	1	4	4
IBM API Connect Microgateway	4	4	4	1
Kong Enterprise Edition	4	4	4	4*
Microsoft Azure API Management	1	1	1	4
MuleSoft Mule	4	2	4	4
NGINX Plus	4	4	4	1
Red Hat 3scale APIcast API Gateway	4	4	4	4
Software AG webMethods API Gateway	4	1	4	4
TIBCO API Exchange Gateway	4	1	4	4
TIBCO Mashery Enterprise	4	1	4	4
TIBCO Project Mashling	4	4	4	1
WSO2 API Manager/API Cloud	4	4	4	1
WSO2 API Microgateway	4	4	4	4

Key:
Fill color correlates to the offering's strength in each listed criterion:
1 = None
2 = Via customization
3 = Via integration with any other product
4 = Yes

* Is on roadmap.
ID: 349440

Source: Gartner (June 2018)

Table 8. Part of DevSecOps Enablement — Deployment Options (Footnotes)

Offering	Notes
Axway API Gateway	■ Axway API Gateway is delivered as a software install, a physical appliance, a virtual appliance (VMware or AMI) and an Axway Cloud service. ■ API Manager is a layered product running on top of API Gateway in all the above form factors. ■ Axway API Analytics is delivered as a software install and as an Axway Cloud service. ■ All components can be deployed in Docker containers.

CA Technologies API Gateway	■ CA API Gateway enables users to deploy to a variety of environments by offering support in multiple form factors:
	  ■ Software
	  ■ Docker container
	  ■ Hardware appliance
	  ■ Virtual appliance
	  ■ AMI
	  ■ Azure VM
	  ■ SaaS (CA API Management SaaS)
	■ The client SDKs are open source.

CA Technologies Microgateway	■ The client SDKs are open source.

IBM DataPower Gateway	■ DataPower Gateway is available in the following form factors:
	  ■ Software (Docker or Linux application), for deployment in cloud and virtual environments
	  ■ Virtual appliance, for deployment in VMware virtualization environments
	  ■ Physical appliance
	■ The IBM API Connect offering, which requires DataPower Gateway, is delivered as SaaS (multitenant and single-tenant) and as a virtual appliance.

IBM API Connect Microgateway	■ API Connect Microgateway is container-ready. ■ A sample Docker file is provided. ■ The user is responsible for creating a Docker container to run the Node.js-based microgateway process.
Kong Enterprise Edition	■ The Kong Cloud offering is in beta.

Offering	Notes
MuleSoft Mule	▪ Mule Kernel, the core of the Mule runtime engine, is open source.
NGINX Plus	▪ NGINIX Plus is available as a software install, a cloud platform image or a Docker container. ▪ NGINX Plus is the freemium version of NGINX OSS. ▪ NGINX Plus can be deployed as a Kubernetes Ingress Controller, and can discover and route traffic to container workloads.
Red Hat 3scale APIcast API Gateway	▪ The APIcast API gateway is open source. ▪ The rest of the 3scale API Management platform will be open-sourced later this year. ▪ Containerized deployment is via container images in Red Hat's Kubernetes-based cloud management platform, OpenShift.
Software AG webMethods API Gateway	▪ The product is not open source. However, Software AG offers free trials of both the cloud and the on-premises versions. ▪ The product provides scripts to "Dockerize" with a single command. It is also available on Docker.
TIBCO API Exchange Gateway	▪ Supported form factors include SaaS, virtual appliance and container (e.g., Docker and Kubernetes).
TIBCO Mashery Enterprise	▪ Supported form factors include SaaS, virtual appliance and container (e.g., Docker and Kubernetes).
TIBCO Project Mashling	▪ Project Mashling is container-ready.
WSO2 API Manager/API Cloud	▪ For containerized deployment, the gateway is available on Docker Hub.
WSO2 API Microgateway	▪ For containerized deployment, the microgateway is available on Docker Hub.
AMI = Amazon Machine Image	

Source: Gartner (June 2018)

Operations Orchestration

Operations automation and controls are foundational to protecting APIs, and are especially important for microservices. Figure 16 and Table 9 assess support for the following DevSecOps orchestration features:

- **Developer Portal With API Catalog:** The vendor provides an API developer portal that includes an API catalog (you can't protect what you don't know you have).

- **All Operations Programmatic:** All administrative and operations functions, including security and identity configurations, can be performed programmatically.
- **Scriptable Operations:** All operations, including identity and security operations, should be scriptable to enable fuller automation.
- **Schema Import and Export:** The vendor supports schema definition generation, import and export (e.g., SOAP, Web Services Deployment Language [WSDL], REST, OpenAPI/Swagger, RESTful API Modeling Language [RAML] and API Blueprint).

Figure 16. Part of DevSecOps Enablement — Operations Orchestration

Part of DevSecOps Enablement — Operations Orchestration

Offering	Developer Portal With API Catalog	All Operations Programmatic	Scriptable Operations	Schema Import and Export†
Amazon API Gateway	3	4	4	4
Apigee Edge	4	4	4	4
Apigee Edge Microgateway	3	4	4	4
Axway API Gateway	4	4	4	4
CA Technologies API Gateway	4	4	4	4
CA Technologies Microgateway	3	4	4	4
IBM DataPower Gateway	3	4	4	4
IBM API Connect Microgateway	3	4	4	4
Kong Enterprise Edition	4	4	4	4
Microsoft Azure API Management	4	4	4	4
MuleSoft Mule	4	4	4	4
NGINX Plus	1	2	4	1
Red Hat 3scale APIcast API Gateway	4	4	4	4
Software AG webMethods API Gateway	4	4	4	4
TIBCO API Exchange Gateway	4	3	4	4
TIBCO Mashery Enterprise	4	3	4	4
TIBCO Project Mashling	3	2	4	1
WSO2 API Manager/API Cloud	4	4	4	4
WSO2 API Microgateway	1	4	4	1

Key:
Fill color correlates to the offering's strength in each listed criterion:
1 = None
2 = Via customization
3 = Via integration with any other product
4 = Yes
† For the Schema Import and Export column:
1 = No standard
4 = Multiple formats
ID: 349440

Source: Gartner (June 2018)

Table 9. Part of DevSecOps Enablement — Operations Orchestration (Footnotes)

Offering	Notes
Amazon API Gateway	■ The developer portal is an open-source toolkit. It supports the ability to import/export APIs using OpenAPI/Swagger 2.0. ■ These schemas can be imported and exported in both JSON and YAML formats, with additional Postman extensions if required.
Apigee Edge	■ Supported protocols include SOAP, WSDL, REST and OpenAPI/Swagger.
Apigee Edge Microgateway	■ APIs and microservices that are managed with Apigee Edge Microgateway can be published to the API catalog that is included as part of Apigee Edge. ■ Supported protocols include SOAP, WSDL, REST and OpenAPI/Swagger.
Axway API Gateway	■ Axway API Gateway supports import and export of SOAP, WSDL and REST-OpenAPI/Swagger. ■ It supports import of REST-RAML via conversion into REST-OpenAPI/Swagger.
CA Technologies API Gateway	■ Supported protocols include SOAP and WSDL. ■ Some REST-OpenAPI/Swagger validation is supported (not full support).
CA Technologies Microgateway	■ The developer portal is provided via CA API Developer Portal. ■ Supported protocols include SOAP and WSDL. ■ Some OpenAPI/Swagger validation is supported (not full support).
IBM DataPower Gateway	■ The developer portal and API catalog are provided via the IBM API Connect offering. ■ DataPower Gateway has built-in support for SOAP, WSDL and REST-OpenAPI/Swagger. ■ Open-source or commercial tools can be used to convert RAML or API Blueprint to OpenAPI/Swagger, which can then be used with the gateway.
IBM API Connect Microgateway	■ REST-OpenAPI/Swagger is supported. ■ Open-source or commercial tools can be used to convert RAML or API Blueprint to OpenAPI/Swagger, which can then be used with the gateway.
Kong Enterprise Edition	■ Supported protocols include OpenAPI/Swagger, RAML and API Blueprint. ■ Converters are available for other formats.
Microsoft Azure API Management	■ Supported protocols include OpenAPI 1.0 and 2.0 (and soon 3.0), WSDL and WADL.
MuleSoft Mule	■ Supported protocols include SOAP, WSDL, REST-RAML and REST-OpenAPI.

Offering	Notes
NGINX Plus	■ NGINX Plus is partially API-enabled. An API exists for custom service discovery integrations (when DNS is not used). This API manages the list of endpoints for each API service. The API allows management of a key-value store that can be used for several API gateway use cases, such as API keys, whitelists/blacklists, and hostname routing. ■ Ansible Roles, Puppet and Chef solutions are available.
Red Hat 3scale APIcast API Gateway	■ The APIcast API gateway can import OpenAPI specifications and RAML. ■ Red Hat offers Apicurio Studio for generation of OpenAPI specifications. ■ OpenAPI specification schemas may be exported from Apicurio Studio as well as from Red Hat Fuse (implementation/app logic).
Software AG webMethods API Gateway	■ Supported protocols include WSDL, OpenAPI/Swagger and RAML.
TIBCO API Exchange Gateway	■ Almost all the tasks that can be performed through the user interface can also be accomplished by using the Mashery platform API to manage API configuration, user management, reporting and I/O Docs. ■ Supported protocols include SOAP, WSDL and REST-OpenAPI/Swagger.
TIBCO Mashery Enterprise	■ Almost all that tasks that can be performed through the user interface can also be accomplished by using the Mashery platform API to manage API configuration, user management, reporting and I/O Docs. ■ Supported protocols include SOAP, WSDL and REST-OpenAPI/Swagger.
TIBCO Project Mashling	■ Project Mashling works with the Mashery developer portal. ■ All functions are available via a CLI, which is scriptable.
WSO2 API Manager/API Cloud	■ Supported protocols include SOAP, WSDL and REST-OpenAPI/Swagger.

CLI = command line interface; WADL = Web Application Development Language

Source: Gartner (June 2018)

Licensing Options

Figure 17 and Table 10 summarize support for different licensing models. Licensing options include, but are not limited to, the following:

- **Subscription License:** A subscription license
- **Support Subscription:** A separate support-only subscription option, usually for open-source offerings

- **Perpetual License:** A one-time license fee
- **Per Processor Value Unit or Core:** Licensing based on the number of processor- or core-equivalents upon which the software is deployed
- **Per Instance:** Licensing based on the number of instances of the software used
- **By Volume:** Licensing based on traffic and/or data volume
- **Per Developer:** Licensing based on the number of developers

Figure 17. License Models

License Models

Offering	Subscription License	Support Subscription	Perpetual License	Per Processor Value Unit or Core	Per Instance	By Volume	Per Developer
Amazon API Gateway	4	1	1	1	1	4	1
Apigee Edge	4	1	4	1	1	4	4
Apigee Edge Microgateway	4	1	4	1	1	4	4
Axway API Gateway	4	1	4	4	1	4	1
CA Technologies API Gateway	4	1	4	1	4	1	4
CA Technologies Microgateway	4	1	4	1	4	1	4
IBM DataPower Gateway	4	4	4	4	1	4	4
IBM API Connect Microgateway	4	1	4	4	1	4	1
Kong Enterprise Edition	4	1	1	1	1	1	4
Microsoft Azure API Management	4	1	1	1	4	4	1
MuleSoft Mule	4	1	1	4	1	1	1
NGINX Plus	4	1	1	1	4	4	1
Red Hat 3scale APIcast API Gateway	4	1	1	4	1	4	1
Software AG webMethods API Gateway	4	1	4	4	4	1	1
TIBCO API Exchange Gateway	1	1	4	4	1	1	1
TIBCO Mashery Enterprise	4	1	1	1	1	4	1
TIBCO Project Mashling	1	4	1	1	1	1	1
WSO2 API Manager	4	4	1	1	4	1	1
WSO2 API Cloud	1	4	1	1	1	4	1
WSO2 API Microgateway	4	4	1	1	4	1	1

Key:
Fill color correlates to the offering's strength in each listed criterion:
1 = No
4 = Yes
ID: 349440

Source: Gartner (June 2018)

Table 10. License Models (Footnotes)

Offering	Notes
Amazon API Gateway	■ Customers pay only for the API calls received and the associated data transfer.
Apigee Edge	■ Licensing is also based on features.
Apigee Edge Microgateway	■ Apigee Edge Microgateway is bundled with Apigee Edge. ■ From a licensing perspective, API calls that flow through the Apigee Edge Microgateway are treated like any other API call that is processed by Apigee Edge.
Axway API Gateway	■ Software installation, virtual appliances and Docker containers are available through both core-based perpetual licenses and subscription licenses. ■ Axway Cloud service is licensed through a volume-based subscription. ■ The on-premises offering is available through a perpetual or subscription license.
CA Technologies API Gateway	■ CA API Gateway is licensed per instance. ■ Per-developer licenses are available for preproduction development environments.
CA Technologies Microgateway	■ CA Microgateway is licensed per instance and sold in bundles of instances. ■ Per-developer licenses are available for preproduction development environments (virtually unlimited number of instances).

IBM DataPower Gateway	■ In stand-alone API gateway use cases, licensing is:
	  ■ Per processor value unit (perpetual and monthly subscription) for cloud and virtual form factors
	  ■ Per instance for the physical appliance form factor
	  ■ Per user for developer usage with IBM support
	  ■ Free for developer usage without IBM support
	■ DataPower Gateway inherits IBM API Connect licensing when used within that integrated offering for complete API life cycle management. API Connect is available:

IBM API Connect Microgateway	■ API Connect MicroGateway is free to use for stand-alone gateway use cases under the Apache License. ■ It inherits IBM API Connect licensing when used within that integrated offering for complete API life cycle management.
Kong Enterprise Edition	■ Kong EE charges a flat fee through an annual subscription for each seat/administrator. ■ Kong CE is OSS and free to use. Note that web-based administration and some plug-ins are not included in the community edition.

Offering	Notes
Microsoft Azure API Management	■ Azure API Management is offered in three tiers: developer, standard and premium.
MuleSoft Mule	■ All MuleSoft solutions are offered via annual subscription. ■ The Mule runtime, deployable as an API gateway either on-premises or in the cloud, is available first as part of a base subscription package. If users need more compute capacity, they are then charged for each additional virtual core. ■ To manage these gateways and analyze traffic, customers can purchase the API Manager and Analytics solution as an add-on to the base subscription package.
NGINX Plus	■ Licensing is available by subscription and per instance. ■ Enterprise licensing options are available for container-friendly and large-volume deployments. ■ Cloud platform images (e.g., AMI) are metered on use.
Red Hat 3scale APIcast API Gateway	■ Unlimited gateways can be deployed with no incremental costs. ■ The free tier allows for up to 5,000 calls per day.
Software AG webMethods API Gateway	■ For cloud customers, licensing is by subscription contract. ■ For on-premises implementations, the gateway is available through either of the following: 1. A traditional perpetual license, where customers incur an upfront license cost and annual maintenance fees of about 20% of the license cost 2. A subscription license, with terms similar to the cloud-hosted service ■ Customers can deploy on-premises and subscription licenses using any combination of on-premises, public cloud or private cloud environments.
TIBCO API Exchange Gateway	■ API Exchange Gateway follows a per-CPU perpetual model.
TIBCO Mashery Enterprise	■ Mashery Enterprise follows a subscription model (support is included).
TIBCO Project Mashling	■ Mashling is provided as open source, under the BSD license. ■ Commercial support for Project Mashling is available as part of TIBCO Mashery Local. One Mashery Local cluster supports up to 10 Mashling instances. A Mashery Local cluster includes one Mashery Local instance that functions as a master instance and any number of Mashery Local slave instances.
WSO2 API Manager	■ API Manager is provided under the Apache License (v.2.0), with a commercial support subscription licensed per JVM instance deployed.
WSO2 API Cloud	■ API Cloud's pricing is based on volume (calls and users) and on feature-based tiers.

Offering	Notes
	■ Additional subscriptions (often lower-tier) typically get purchased for nonproduction environments.
WSO2 API Microgateway	■ API Microgateway is provided under the Apache License (v.2.0), with a commercial support subscription licensed per JVM instance deployed.
JVM = Java Virtual Machine	

Source: Gartner (June 2018)

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"A Guidance Framework for Evaluating API Management Solutions"

"Protecting Web Applications and APIs From Exploits and Abuse"

"Modern Identity and APIs: Mobile, OpenID Connect, OAuth, JSON and REST"

"Best Practices for Using the Evolving OAuth 2.0 Framework"

"Single Sign-On in Native Apps and Modern Web Apps"

"Building Identity Into Microservices"

"Evaluation Criteria for Access Management"

"A Guidance Framework for Designing a Great API"

"Assessing Microservices for Agile Application Architecture and Delivery"

"Selecting a Cloud Platform for DevOps Delivery With Microservice Architecture"

"Choosing an Architecture for Managing APIs and Services"

"Magic Quadrant for Full Life Cycle API Management"

"Critical Capabilities for Full Life Cycle API Management"

Evidence

This report is based on a Gartner study of select API gateway and identity gateway vendors, conducted in January and February 2018. It also reflects lessons learned through client inquiries and interviews on this topic.

For the vendor study, Gartner interviewed and surveyed 13 vendors. The list includes the following mix of incumbent enterprise integration software vendors, cloud vendors and IAM vendors: Amazon Web Services, Apigee, Axway, CA Technologies, IBM, Kong, Microsoft, MuleSoft, NGINX, Red Hat 3scale, Software AG, TIBCO Software and WSO2.

Vendors included in this comparison consist of all of the vendors in the most recent Leader quadrant of the Gartner "Magic Quadrant for Full Life Cycle API Management." In addition, we included some of the vendors positioned near the boundaries of the Leaders quadrant, because we frequently receive inquiries about them. We also included NGINX, an open-source web program on which several other offerings are based. Note also that some vendors declined to participate in the survey on which this research is based.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp