IMPERVA®

SOLUTION BRIEF

Enabling and Securing Digital Business in API Economy

Protect APIs Serving Business Critical Applications

40 percent of the world's web applications will use an API interface

Most enterprises today rely on customers accessing their applications to conduct daily business. These enterprises know by now that application programming interfaces (APIs) are becoming more common than ever before to enable communication between applications and end users. Even though they are working behind the scenes, APIs are ubiquitous – they help to deliver sports updates, post online messages, order food – enabling everything online.

To stay competitive, businesses need to publically expose and rely on API calls to applications that serve business-enabling data to consumers. Leading industry analysts expect that by 2019, around 40 percent of the world's web applications will use an API interface which is almost a three times increase compared to its usage in 2015.

The increased usage can also be attributed to applications moving into public and private cloud infrastructure because the cloud's agility, resiliency and scalability drives business growth. The other driving factors for increased usage of APIs in a changing application development environment are:

- Rise of DevOps
- Micro-services architecture
- Containers
- Serverless architecture

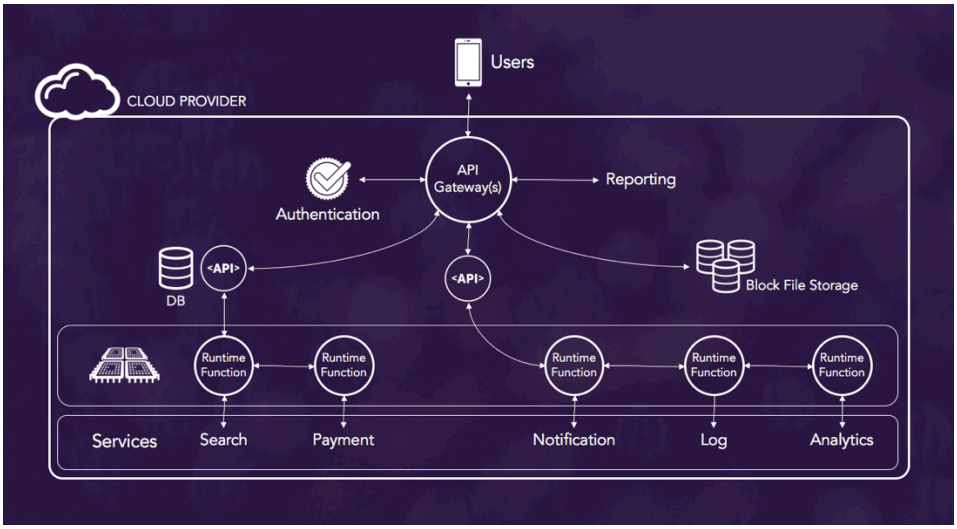

Figure 1: Serverless, Micro-services architecture

More and more IT groups are adopting approaches such as DevOps and micro-services architectures

More and more IT groups are adopting approaches such as DevOps and micro-services architectures, as well as supporting technologies including cloud computing, containers and automation toolchains and frameworks.

Within this new API/application landscape and software development security becomes more challenging as the number of touchpoints and integrations increase. Cybercriminals are increasingly turning their attention to security gaps and vulnerabilities in modern software. Given the speed and volume of API adoption today and the greater complexity of the environment, it's never been more important to secure your applications and data.

Understanding Application Programming Interfaces

APIs at a glance

Application programming interfaces (APIs) aren't new, but they are increasingly important for exposing specific internal functions of a service or application to the outside world. APIs are essentially plug-and-play services that enable different services, applications and platforms to communicate with each other in real time. The popularity of micro-services architecture is driving increased usage and exposure of APIs because all micro-services use APIs to communicate with other services and applications.

Need to provide data to an ecosystem of partners? That's what an API is for.

API economy

APIs are essential today for companies looking to monetize data and services to create new revenue streams. Need to provide data to an ecosystem of partners? That's what an API is for. The API economy, as it's being called, refers to using APIs to deliver new digital products and services to the market and enable new business models and channels.

API gateway

An API gateway establishes a single entry point for all requests coming from clients, insulates the clients from how an application may be partitioned into micro-services, and enables clients to retrieve data from multiple services with one request.

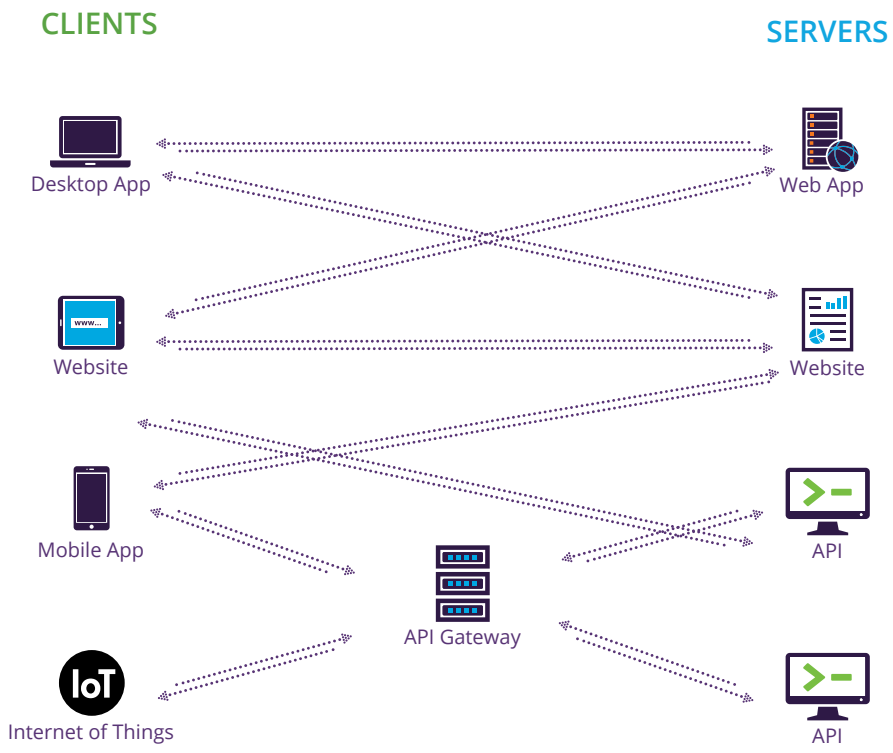

Figure 2: Clients accessing APIs through API Gateway

Security and APIs

It's possible for attackers to reverse-engineer an API by examining client code

Simply put, APIs are an additional attack vector for cybercriminals and can make your micro-services and other endpoints vulnerable to a full range of web application attacks. It's possible for attackers to reverse-engineer an API by examining client code or simply by monitoring communications.

API gateways provide a mediation layer to authenticate and route API calls. As APIs are exposed to more and more clients, they are exposed to a variety of cyber attacks that API gateways cannot stop, including:

DDoS attack can cause quite a disruption to API-fronted web applications.

- **Denial of service attacks:** API-fronted web applications are exposed to bot and DDoS abuse – a poorly written API could use up a lot of compute resources if it starts receiving invalid inputs. In general, a DDoS attack can cause quite a disruption to API-fronted web applications.
- **Exploits and technical attacks:** It's possible for attackers to simply inject malicious content that could lead to exploits. Such technical attacks could include poisoning of JSON web tokens, attempts to light up traditional SQL injection or getting a malicious JS code to execute behind the scenes, amongst many others.
- **API parameter tampering:** One of the most common exploit methods used by hackers is to probe into application security defenses by tampering input parameters (fields). With APIs, such tampering could simply expose a poorly written API to reveal sensitive data.

- **Man in the middle attacks:** An unencrypted connection between the API client and the API server can expose a lot of sensitive data to hackers. Since APIs are becoming a preferred vehicle for data exchange with the easy to use JSON format, an unsecured transmission is an open invitation for data theft.
- **Session cookie tampering:** Attacks can attempt to tamper cookies to either bypass security or to send false data to application servers. While session cookie tampering is a well-known channel for attacking traditional web applications, it is equally relevant for APIs.

As another potential attack vector, API gateways need layered security control and defense.

- **Access violation:** Most Internet of Things (IoT) devices are designed to communicate to their corresponding enterprise servers using the API channel. These IoT devices in some cases authenticate themselves at the API server using client certificates. If a hacker gets control over an API from the IoT endpoint, they could easily re-sequence the order of APIs and cause data leaks or undesired operations.

Many API gateways do API authentication and validation in some form, but that is not enough to stop the application attacks that are mentioned above. As another potential attack vector, API gateways need layered security control and defense. A WAF on the front end helps with access control, bot and DDoS protection, threat detection and filtering.

WAF deployed in front of API resources protects core applications by validating and monitoring API traffic.

Securing APIs with Web Application Firewalls

WAF deployed in front of API resources protects core applications by validating and monitoring API traffic, and leverages WAF features like profiling and content inspection to identify and protect against malicious activity. This enables the full range of WAF features such as rate-limiting, session validation, user tracking, client certificate validation, protocol validation, reputation and community services.

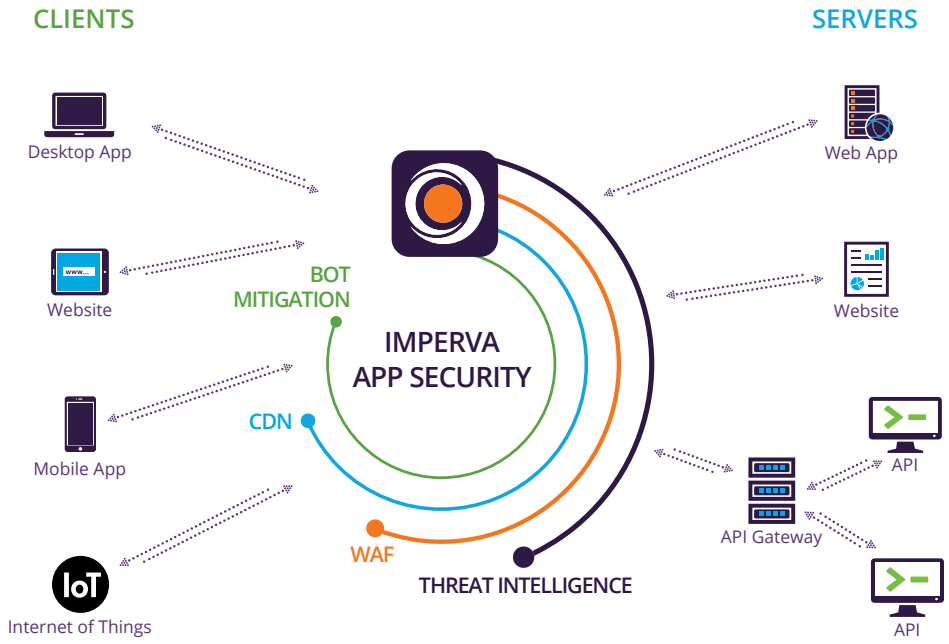

Figure 3: Protecting applications, websites and APIs

Imperva API Security provides a layer of monitoring and protection over the use of APIs in your network. API Security feature set includes the following:

Blocks malicious bot activity and DDoS attacks

As APIs represent a gateway to your computing resources, malicious users can attempt to use this gateway to probe your network and attempt to run automated (bot) attacks. Imperva App Security offers a number of tools to block malicious bot activity. This is done using various mechanisms such as identifying and blocking traffic from malicious IP addresses, blocking traffic from geographic locations which are known to be the source of malicious traffic, and by configuring policies that set rate limits.

Protects APIs against exploits and technical attacks

Imperva WAF can be configured to inspect API content and defend against OWASP Top 10 attacks such as Cross-Site Scripting (XSS) and SQL Injection (SQLi), it also utilizes signatures for attacks specific to these content types, such as XXE.

API Request Profiling protects against parameter tampering

Protects against parameter tampering and malicious fields

Imperva SecureSphere API Request Profiling protects against parameter tampering and malicious fields by profiling API calls and blocking malformed calls, including JSON and nested parameters, as well as inspects requests for compliance.

SecureSphere learns all URLs and their parameters as part of the learning process of SecureSphere profiling. Open APIs can be used to configure profiles reducing the time and increasing the scalability of profiling API URLs.

Enforces API Encryption

Imperva WAF can prevent unauthorized access to your organization's computing resources when working in Reverse Proxy (KRP, TRP) by enforcing TLS communication between clients and servers. This can be useful when you have HTTP-only APIs and want to add encryption to a single point. Additionally, you can enforce TLS versions and which ciphers are being used.

Protect session cookies

Imperva's cookie protection provides protection against improper session handling/ session management and tracking. Session Cookie protection for API security uses standard WAF Cookie Protection.

Access control by tracking API users with client certificates

Imperva SecureSphere learns a web application's login URLs as part of the process of building the Web application profile. When a Web application user successfully authenticates to the application, SecureSphere associates the Web application user name with an HTTP session and IP address, and tracks the user throughout the duration of the session.

Securing APIs requires applying the same application security best practices

Today's modern services are extensively using public APIs and making them an attractive target for cybercriminals looking to gain access into your environment. Securing APIs requires applying the same application security best practices as in the past, but using right solutions built to handle an API environment and accompanying threats. Imperva application security solutions help you to securely build DevOps and Micro-services architecture.

Contact us today to find out how Imperva solutions can integrate into your DevOps workflow and protect your APIs, applications and data from cyber threats.