



Gartner Webinars

Gartner equips leaders like you with indispensable insights, advice, and tools to help you achieve your most pressing objectives

Gartner[®]

Enhance your webinar experience



**Ask a
Question**



**Download
Attachments**



**Share This
Webinar**

API Security: Protect your APIs from Attacks and Data Breaches

  Connect with Gartner



Mark O'Neill

VP Analyst



Dionisio Zumerle

VP Analyst



By 2022, API abuses will move from an infrequent to the most frequent attack vector, resulting in data breaches for enterprise web applications.

Source: "API Security: What You Need to Do to Protect Your APIs" (G00404900)

API Security Flaws Can Result in Data Breaches

CSO
FROM IDG

Home > Security

SALTED HASH- TOP SECURITY NEWS
By [Steve Ragan](#), Senior Staff Writer, CSO

About | Fundamental security insight to help you minimize risk and protect your organization

NEWS

API flaws said to have left Symantec SSL certificates vulnerable

Amazon's Ring Neighbors app exposed users' precise locations and home addresses

Zack Whittaker @zackwhittaker / 10:00 AM EST • January 14, 2021

Comment

USPS exposes 60M customer records via a leaky API

BY DUNCAN RILEY

Instagram's leaky API exposed celebrities' contact details

customer data

to bad API

API Leaks Data for

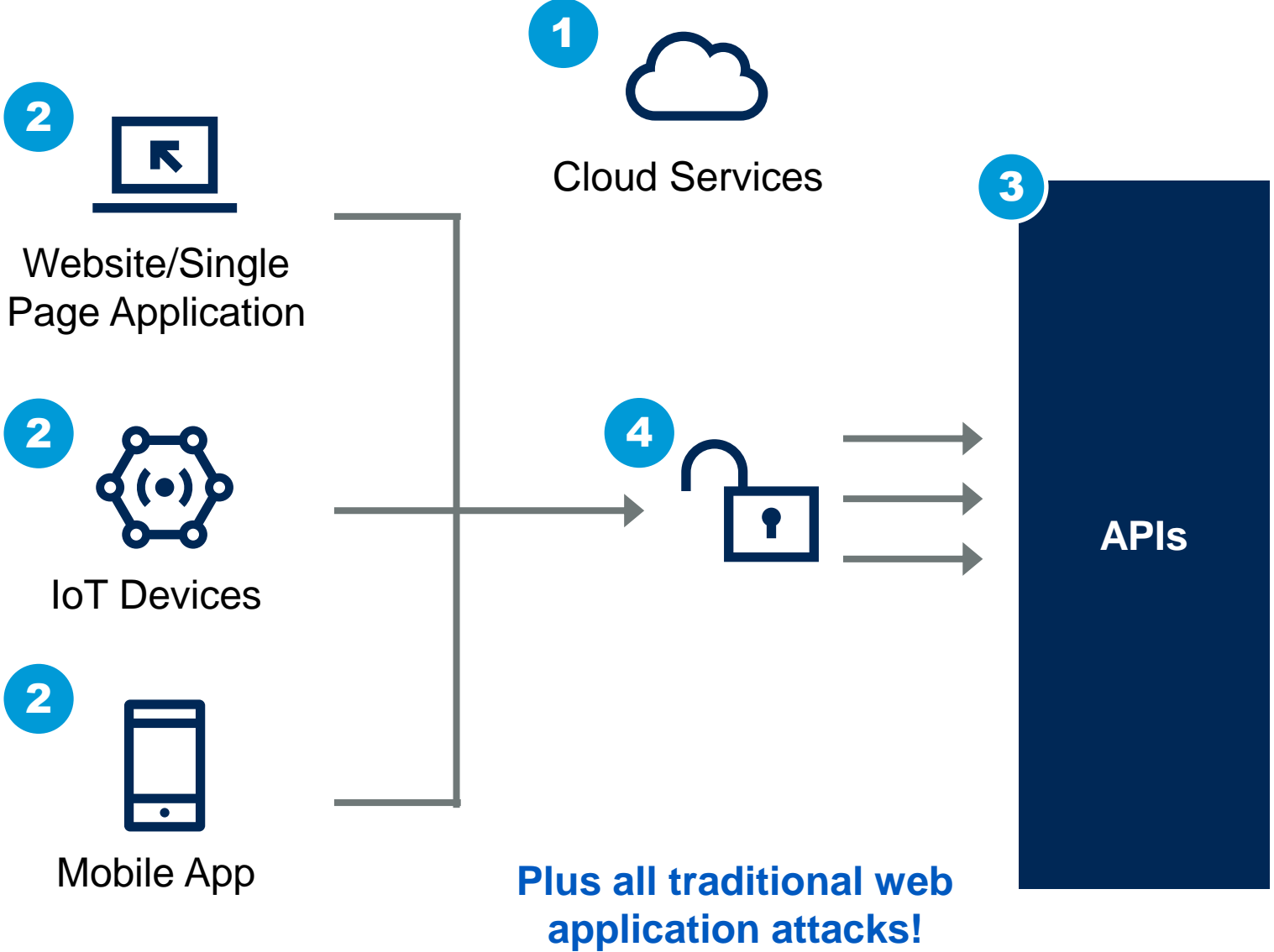
er Being Outed by Researcher

Gartner

Key Issues

1. What are the problems with API security?
2. How can APIs be secured?
3. What products help with API security?

How Are APIs attacked?

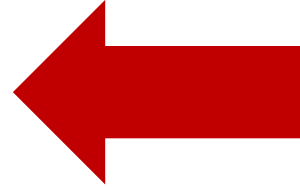


Key:

- 1** Unsecured API keys in repositories and storage
- 2** Hard-coded credentials (incl. API Keys) in applications
- 3** API logic flaws
- 4** Sniffed API calls

OWASP API Security Top 10

1. Broken object level authorization
2. Broken authentication
3. Excessive data exposure
4. Lack of resources and rate limiting
5. Broken function level authorization
6. Mass assignment
7. Security misconfiguration
8. Injection
9. Improper asset management
10. Insufficient logging and monitoring



/patient/333555

What happens if you increment that number?

Key Issues

1. What are the problems with API security?
- 2. How can APIs be secured?**
3. What products help with API security?

Polling Question

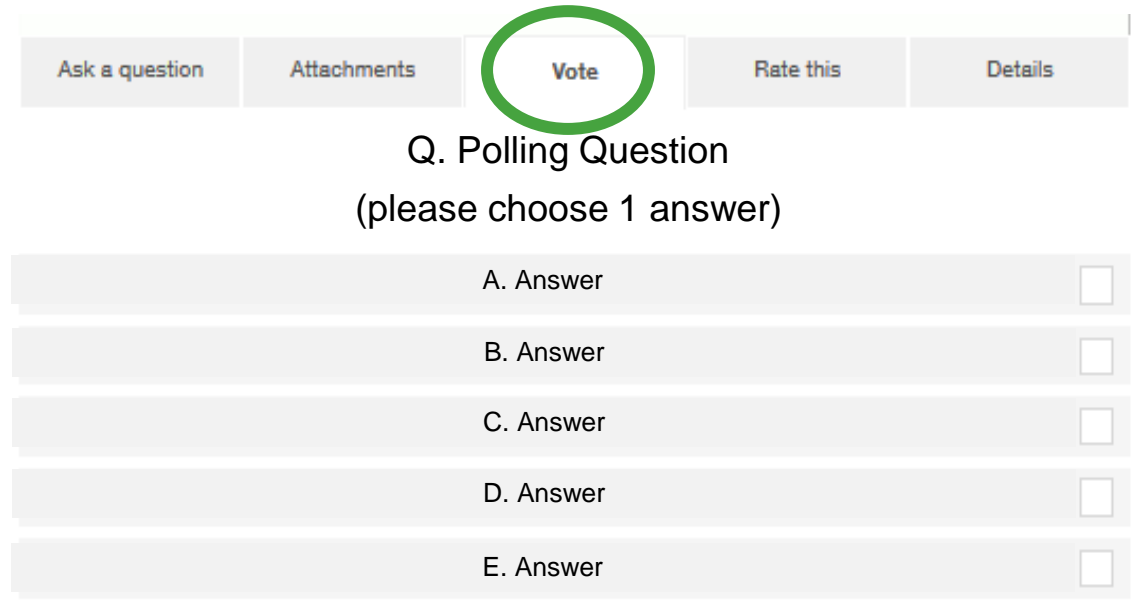
Who is primarily responsible for API security in your organization?

- A. Application Developers
- B. Security Team
- C. API Team
- D. Integration Team
- E. Nobody

How to participate in our polling

If you are in full screen mode – click Esc
The poll question is on the “Vote” tab.
Please click the box to make your selection.
Upon voting you will see the results.

Thank you!



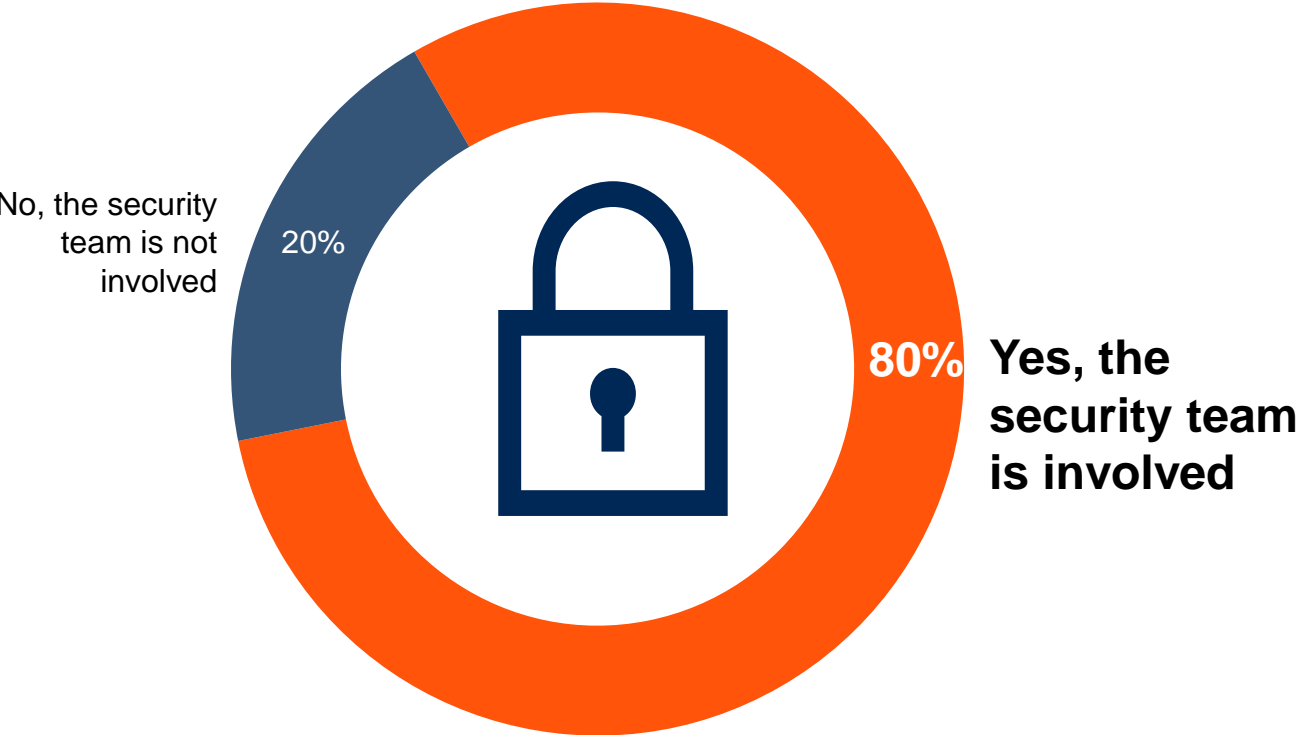
The screenshot shows a navigation bar with five tabs: "Ask a question", "Attachments", "Vote", "Rate this", and "Details". The "Vote" tab is highlighted with a green circle. Below the tabs, the question "Q. Polling Question" is displayed, followed by the instruction "(please choose 1 answer)". There are five answer options, each with a checkbox:

- A. Answer
- B. Answer
- C. Answer
- D. Answer
- E. Answer

Including your Security Team in API Strategy

Involvement of Security Team in API Strategy

Percentage of Respondents



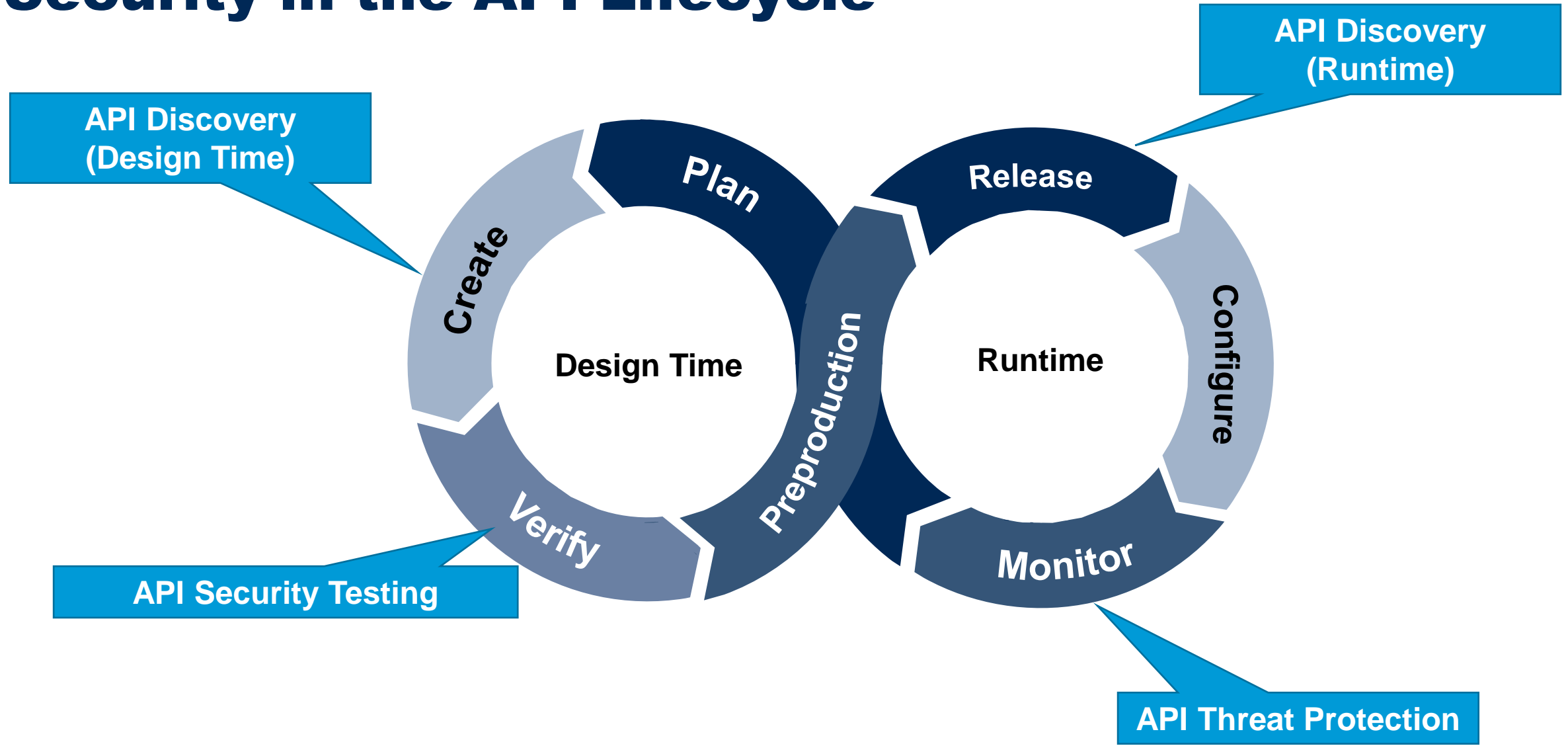
	Use API management solution	Don't use API management solution
Base	66	32
Yes	88%	66%
No	12%	34%

Gartner Research Circle Members; Excludes 'Don't know'
 Q05. Is your security team involved in your organization's API strategy?
 SOURCE: Gartner Research Circle API Usage and Strategy

Statistically significant difference @ 95%

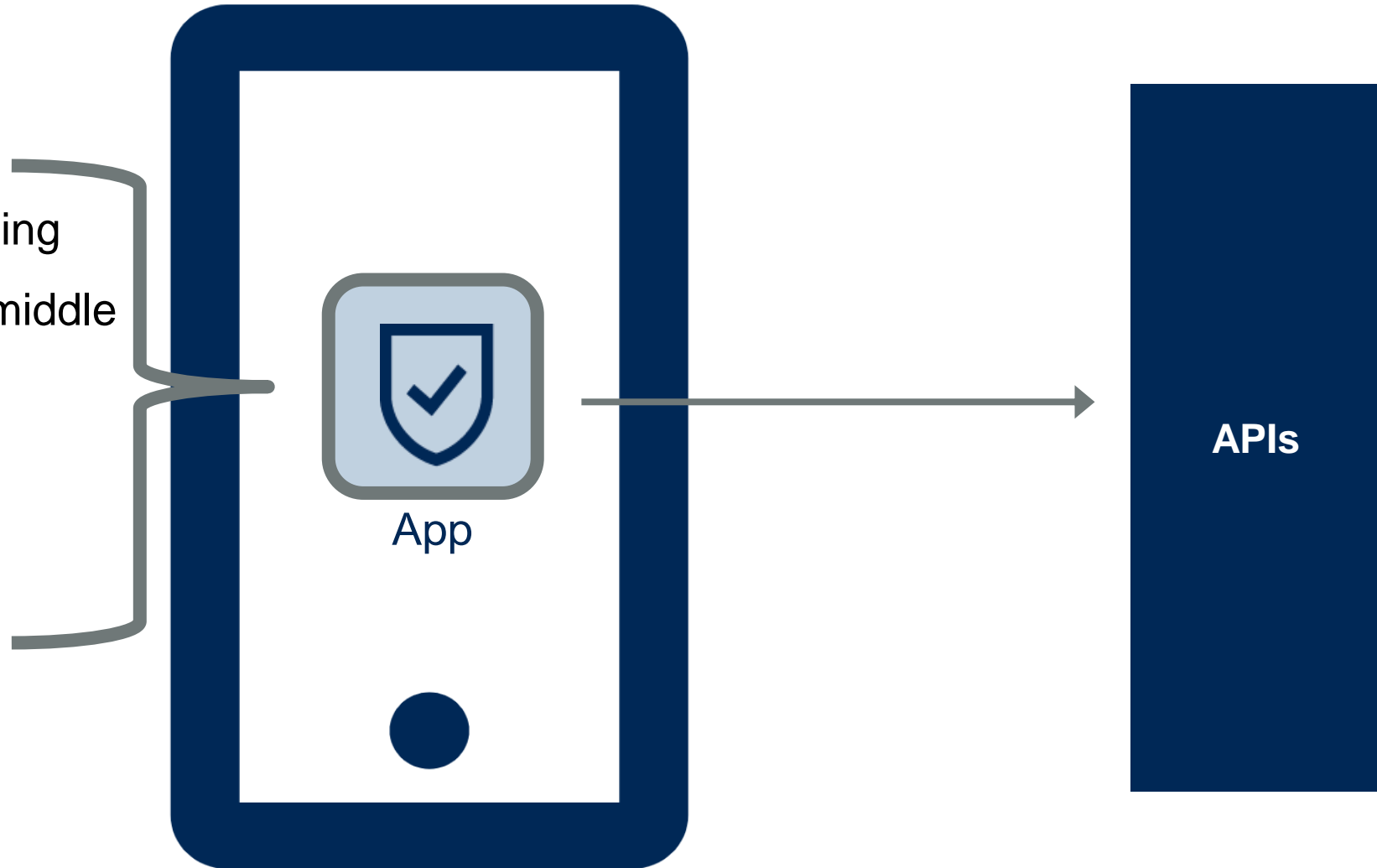


Security in the API Lifecycle



API Security with Mobile and Client-Side Apps

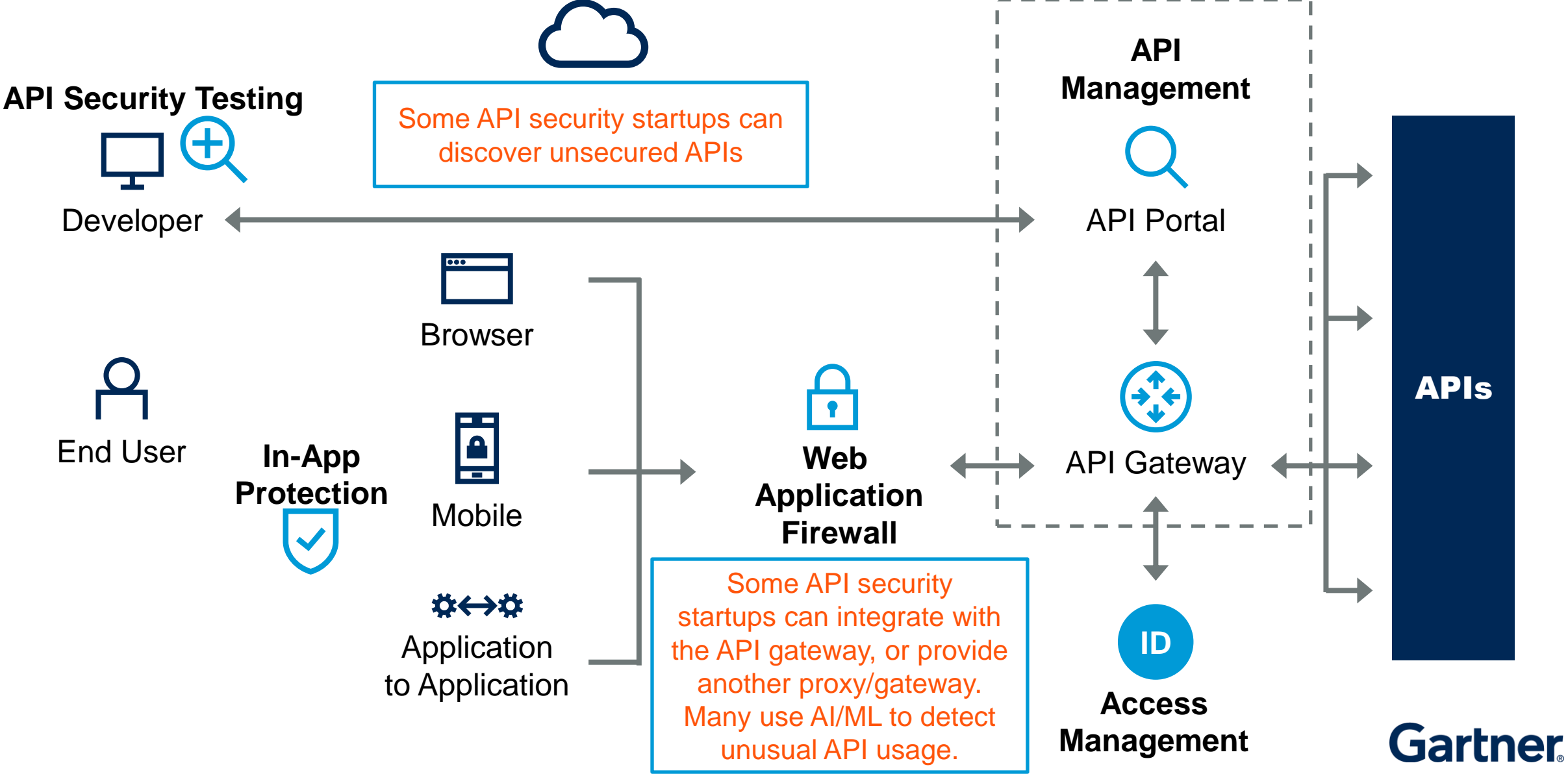
- Avoid credential hardcoding
- Protect from man in the middle attacks
- Verify the environment



Key Issues

1. What are the problems with API security?
2. How can APIs be secured?
3. What products help with API security?

Delivering API Security

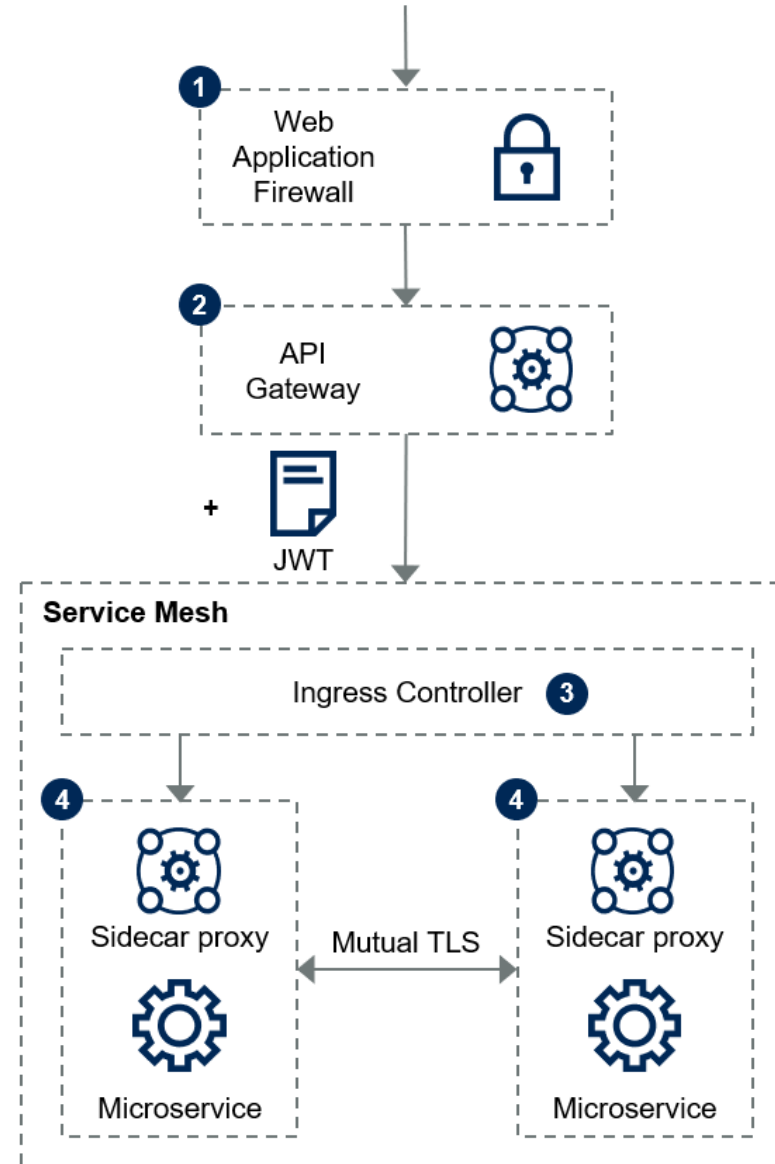


Scenario: Microservices

Key:

↓ North-South ↔ East-West

- 1 Web Application Firewall detects and blocks attacks
- 2 API Gateway authenticates API client, then inserts tokens for identity and attribute propagation
- 3 Ingress Controller routes traffic to microservices and performs load-balancing
- 4 Sidecars enforce fine-grained authorization and secure microservice-to-microservice traffic



API Security Startups

Discovery of
“shadow APIs”



Monitoring and
anomaly detection



Runtime Protection

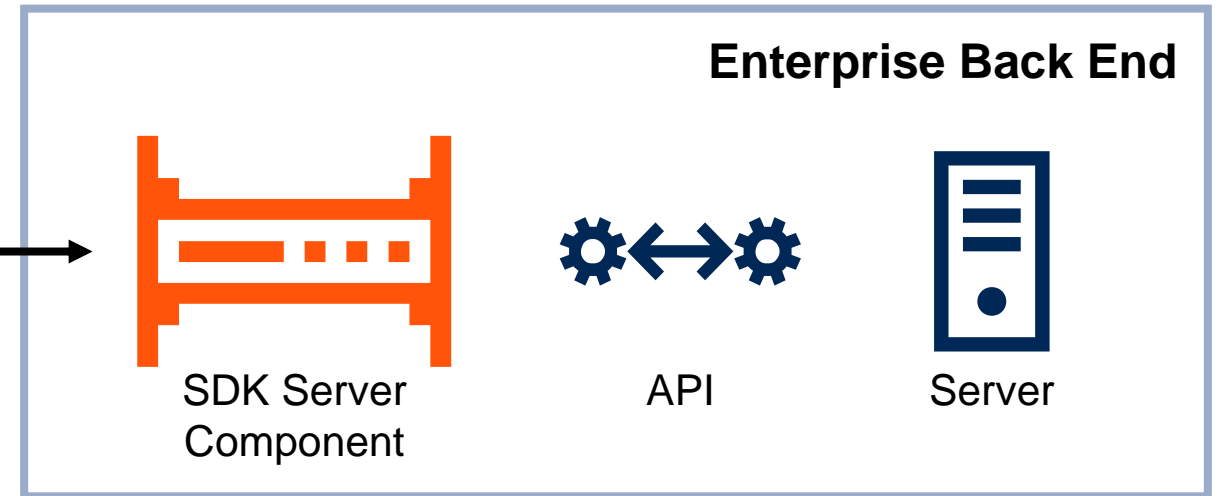


- Sample vendors:

- 42 Crunch, Aiculus, APIsec, Cequence Security, CloudVector (Imperva), Curity, Data Theorem, ForAllSecure, Invision, Neosec, Noname Security, Salt Security, Spherical Defence, Stackhawk, Traceable.

Scenario: API Scraping Protection

Device-Binding
Transaction Signing
Jailbreak/Root Detection
Human Interaction Detection



Used to counter DDoS, API scraping and fraudulent attacks

Sample Vendors: Approov, F5, Imperva, PerimeterX

Putting it all together

1. **Discover:** Inventory APIs that have been delivered, or are in the development process. APIs consumed from third-parties should also be included.






2. **Analyze:** Observe your API usage. Learn what “normal” is for API behavior.



3. **Secure:** Create a policy to secure your APIs.



Three Sides of API Security

	 API Security Testing	 API Protection	 API Access Control
Key functionality	Identification of API security flaws and vulnerabilities	Content validation, threat detection, traffic throttling	Authentication, authorization, identity propagation
Key technologies used	Dynamic application security testing (DAST), fuzzing, static application security testing (SAST)	Attack signature, reputation-based control, anomaly detection, OAS message validation	OAuth 2.0, OpenID Connect, JSON Web Tokens
Product categories	Application security testing tools, specialized API security platforms	Web application firewalls, API management, specialized API security platforms.	API management, access management software, IDaaS.

Your API Security Building Blocks

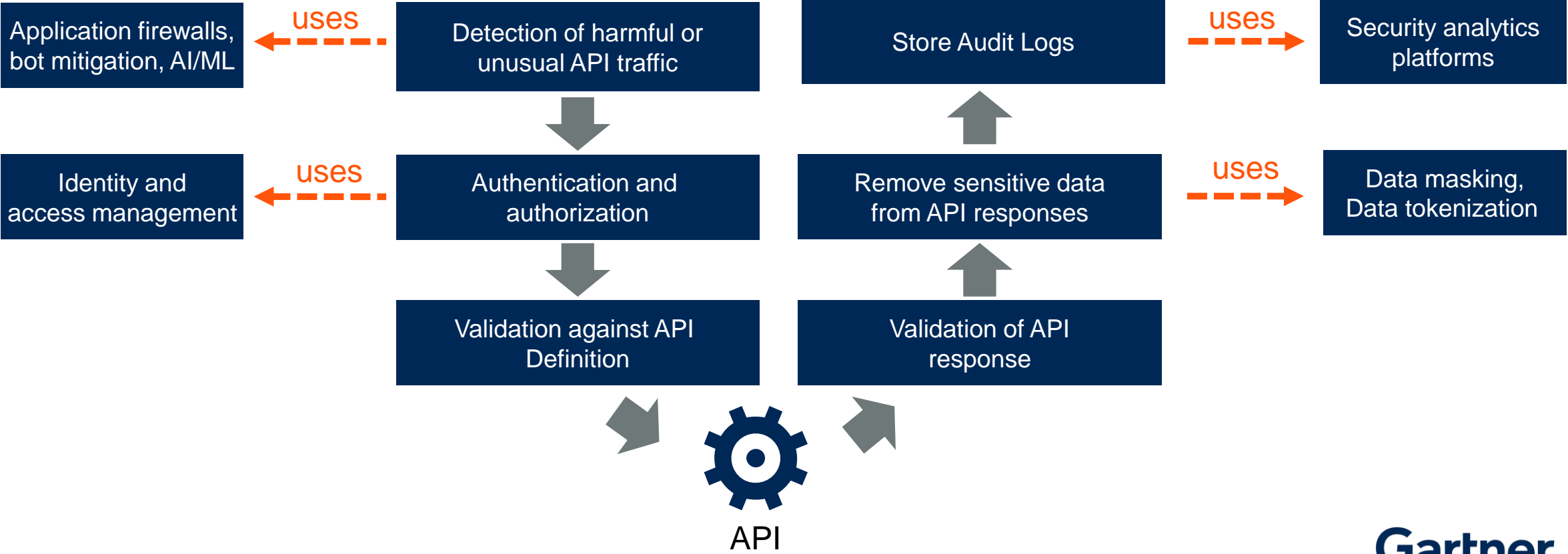
Authentication of the API client (e.g., mobile app)	JSON/XML element encryption	Quota management/ Traffic throttling
Content inspection	Content validation (JSON schema, XML schema)	Tokenization of sensitive information (e.g., patient number)
Automated attack/Bot detection	Usage plan management	Data transformation
Store audit logs	Digital signature	API key authentication
Fine-grained authorization	OAuth scope management	Transport security (TLS/SSL)
Integration with access management	XML/SOAP security (WS-security, etc.)	Alerting (including to SIEM)



Example Policy for API Security



Client Application



Recommendations

- ④ Include your security team in your API platform team
- ④ Consider the whole picture for API security, not just an API gateway
- ④ Think “North South” as well as “East West” for API security

Ask your questions



The image shows a user interface for asking a question. At the top, there are four tabs: 'Ask a question', 'Attachments', 'Rate this', and 'Details'. The 'Ask a question' tab is highlighted with an orange border, and an orange arrow points to it from the left. Below the tabs, the text 'Ask a question' is displayed. Underneath is a large text input field with the placeholder text 'Type your question here...'. At the bottom right of the form, there is a 'Send Question' button, which is also highlighted with an orange border and has an orange arrow pointing to it from the left.

Gartner Security & Risk Management Summit

Gartner®

22 – 23 February 2021 | Virtual (GST)
17 – 18 March 2021 | Virtual (IST)
23 – 24 March 2021 | Virtual (AET)
29 Nov – 1 Dec 2021 | London, UK
20 – 22 September 2021 | Orlando, FL
6 – 8 October 2021 | Tokyo, Japan

Hear independent experts on what matters most now and how to prepare for what's ahead. You'll learn how to create the security and integrated risk management plans you need to give your organization the freedom to grow and innovate with confidence.

Learn more: gartner.com/conf/security

Register with code **WEBINAR** for an exclusive discount.

At this year's conference, you'll learn how to:



Design secure architectures and technical solutions to support digital business objectives



Adapt your data privacy management program to keep pace with rapidly developing regulations



Understand the latest trends in cybersecurity, cloud security, application security, data security and related technologies

Is Open-Source Software More Secure Than Proprietary Software?

Quick answer for product, IT and software engineering leaders to understand the real-world realities of open-source software.

[Download the Research](#)



Gartner[®]

Keep learning



@Gartner_IT



Gartner for IT

Gartner can help you achieve your most critical priorities

Essential insights and advice for every
leader across the enterprise.

[Contact Us](#)

U.S.: 1 800 213 4848

International: +44 (0) 3331 306 809

Get more Gartner insights



Download the research slides



View upcoming and on-demand Gartner webinars
at gartner.com/webinars



Rate this webinar