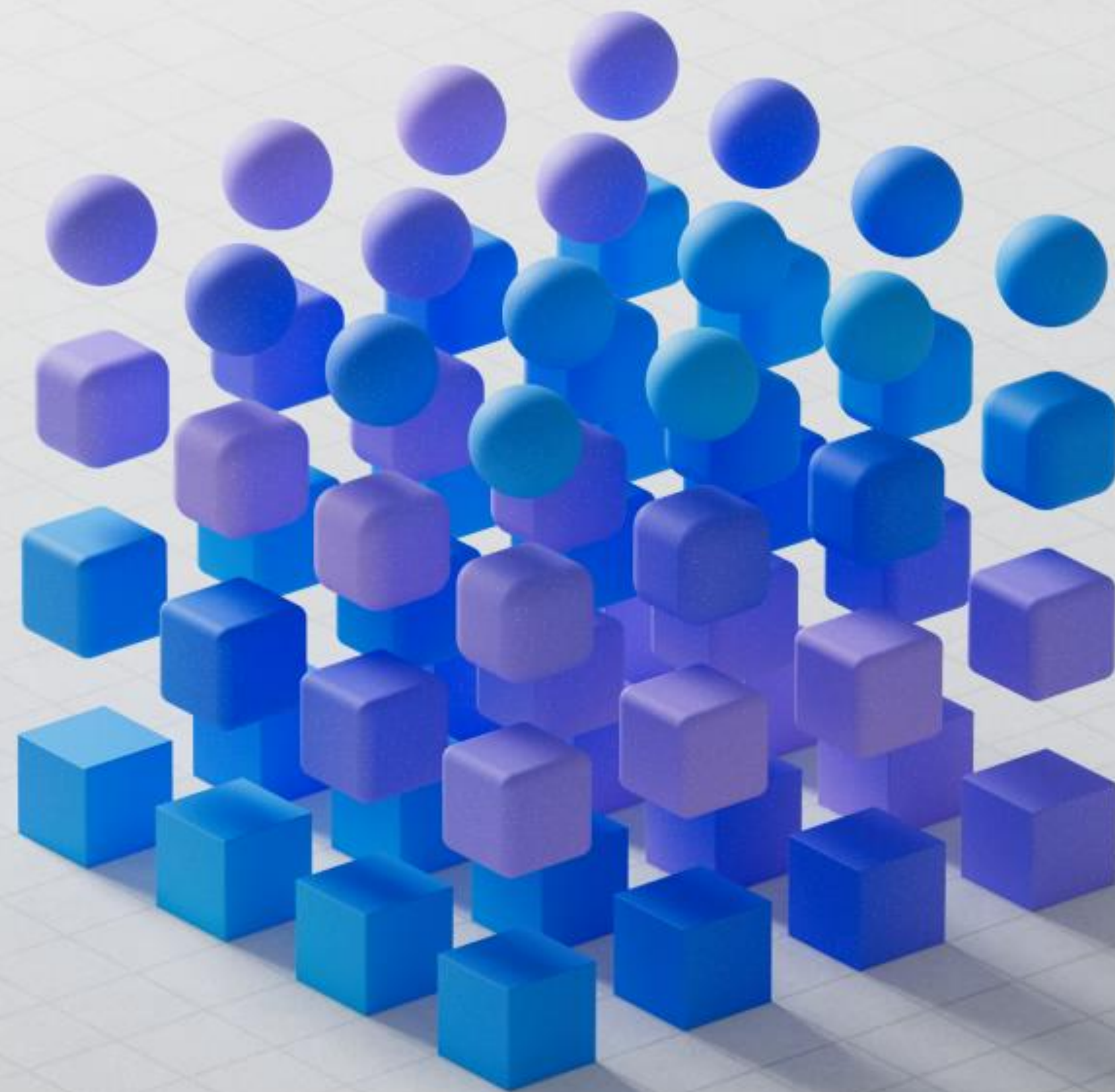




Azure Developers

APIs in Action

February 28, 2024





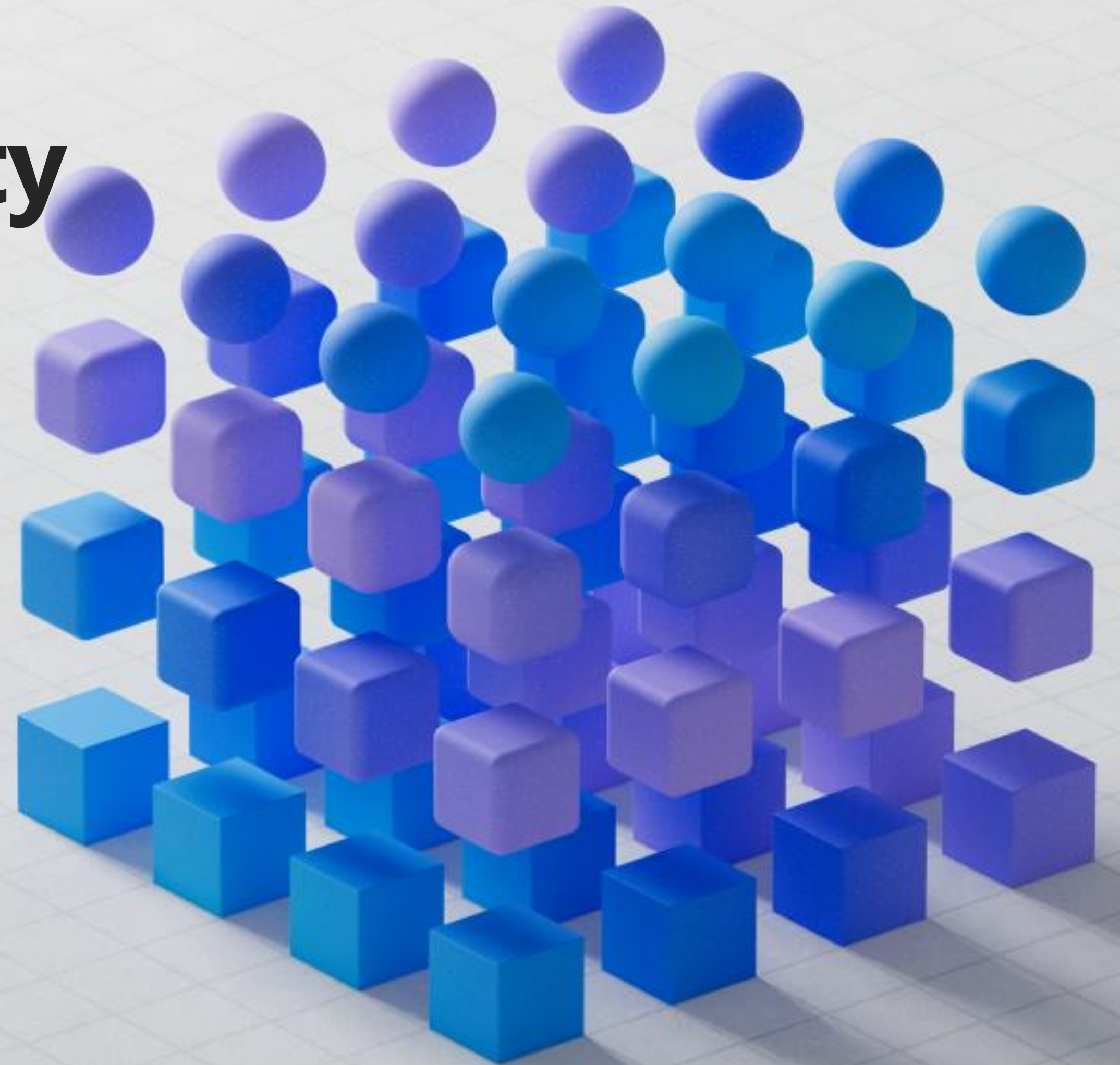
Microsoft

APIs in Action, February 2024

Enhance your API security posture with Microsoft Defender for APIs



Massimo Crippa



API attacks are on the rise

APIs are everywhere



83% of the internet traffic is driven by APIs¹

APIs data breaches has grown



90% of web applications will expose attack surfaces via APIs²

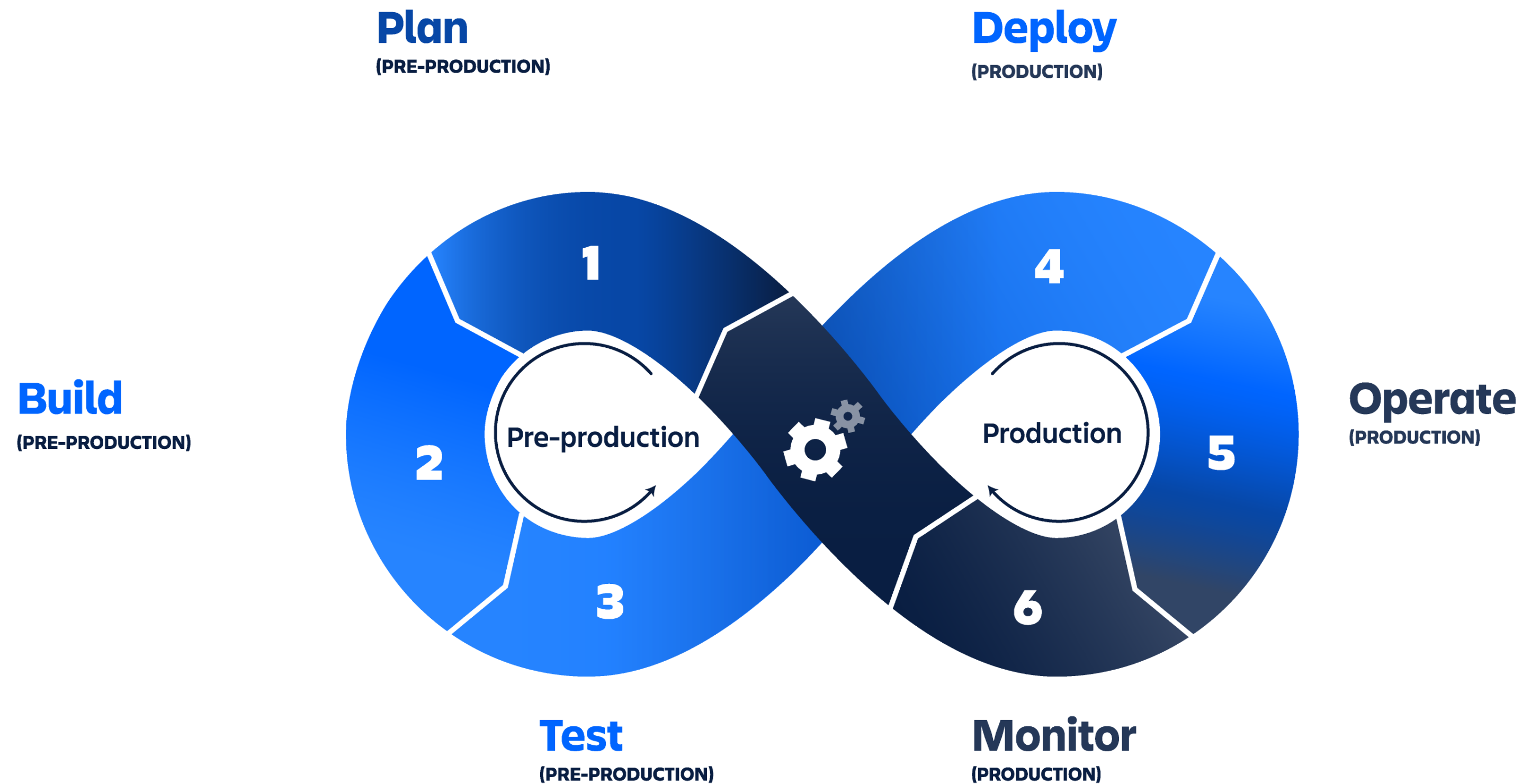
API security has emerged as a significant business issue



59% have experienced application rollout delays resulting from security issues identified in APIs³

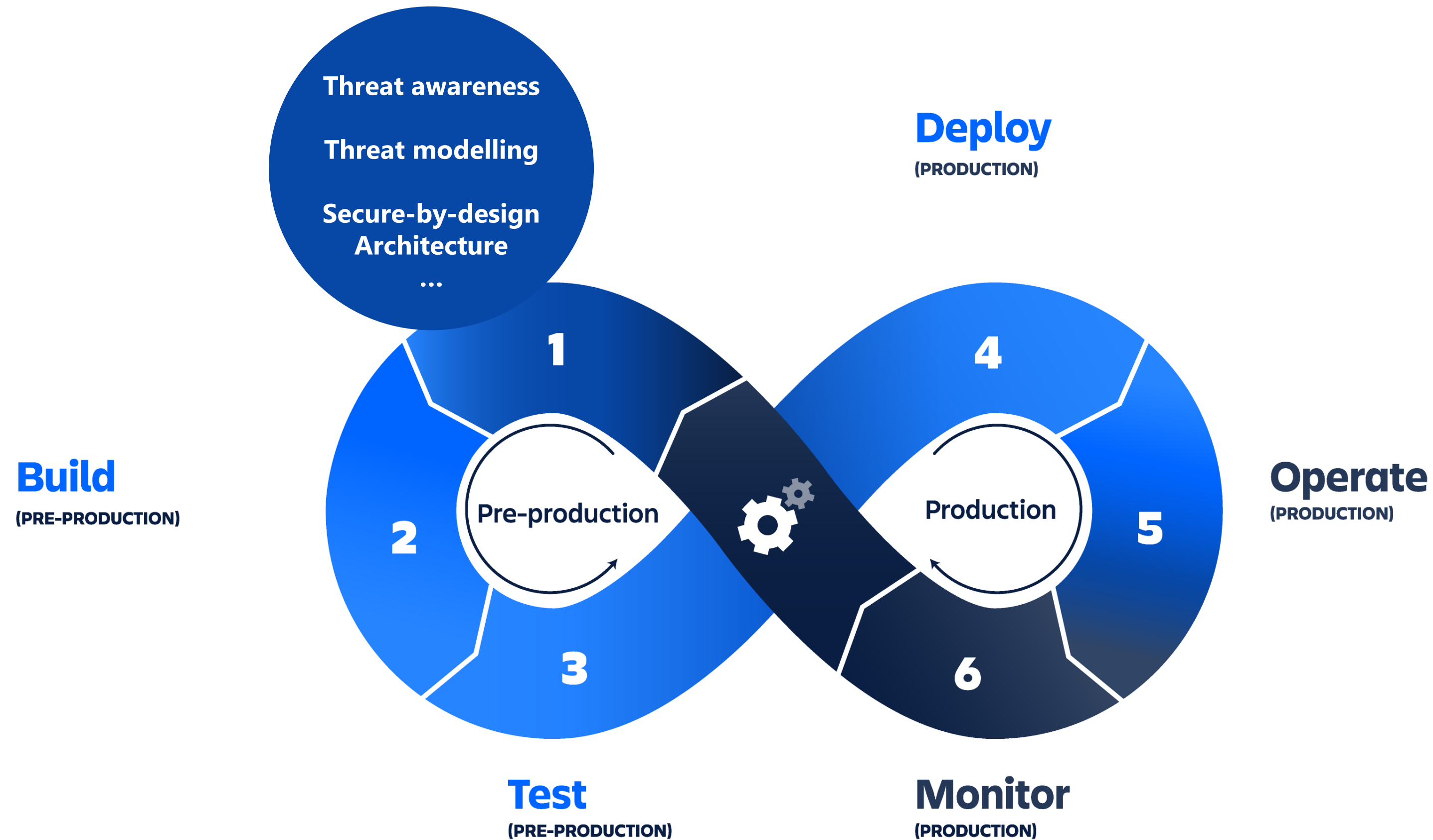
Security is the first concern of every enterprise

Bring together preventive and runtime security models



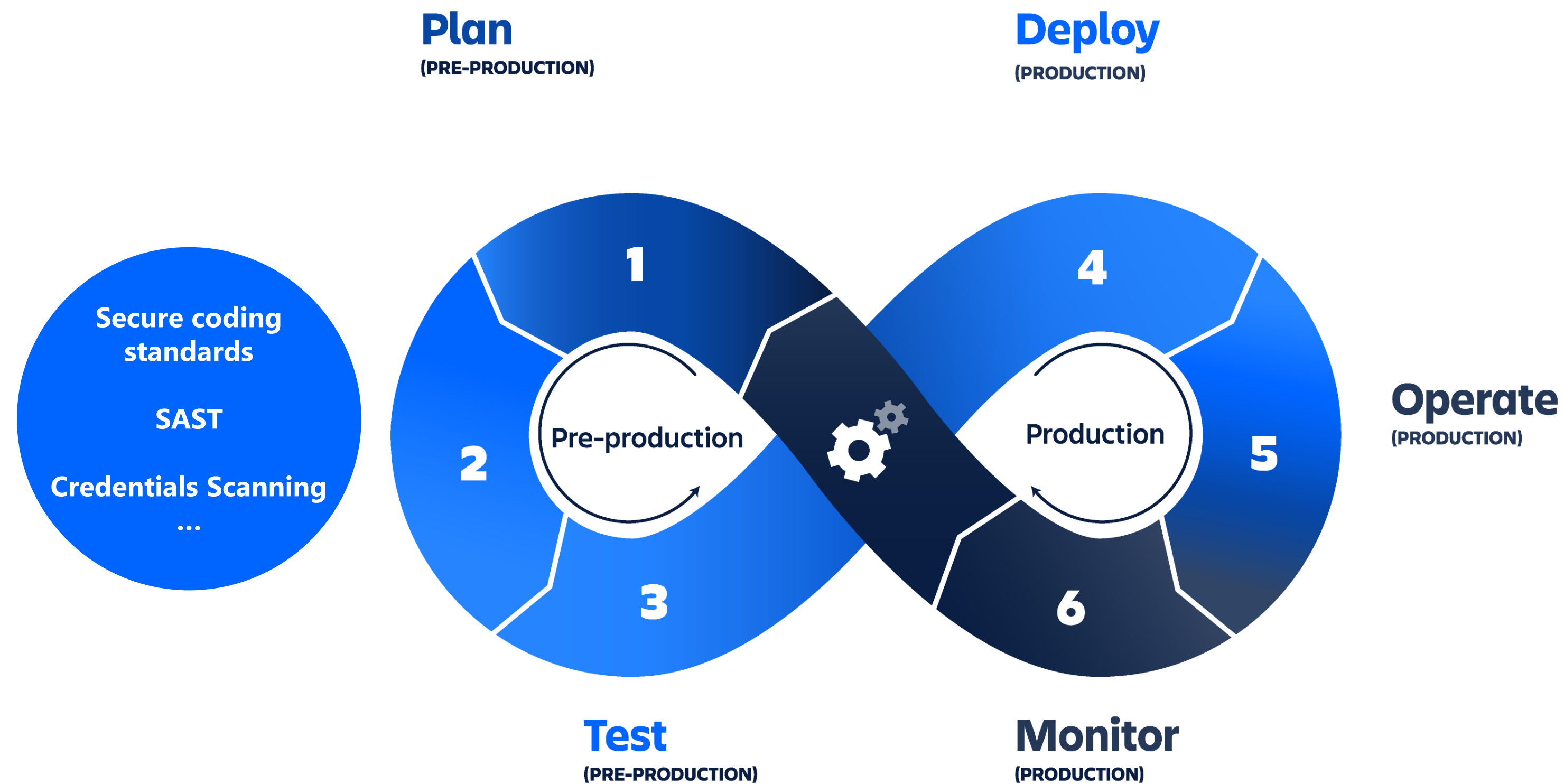
Security is the first concern of every enterprise

Bring together preventive and runtime security models

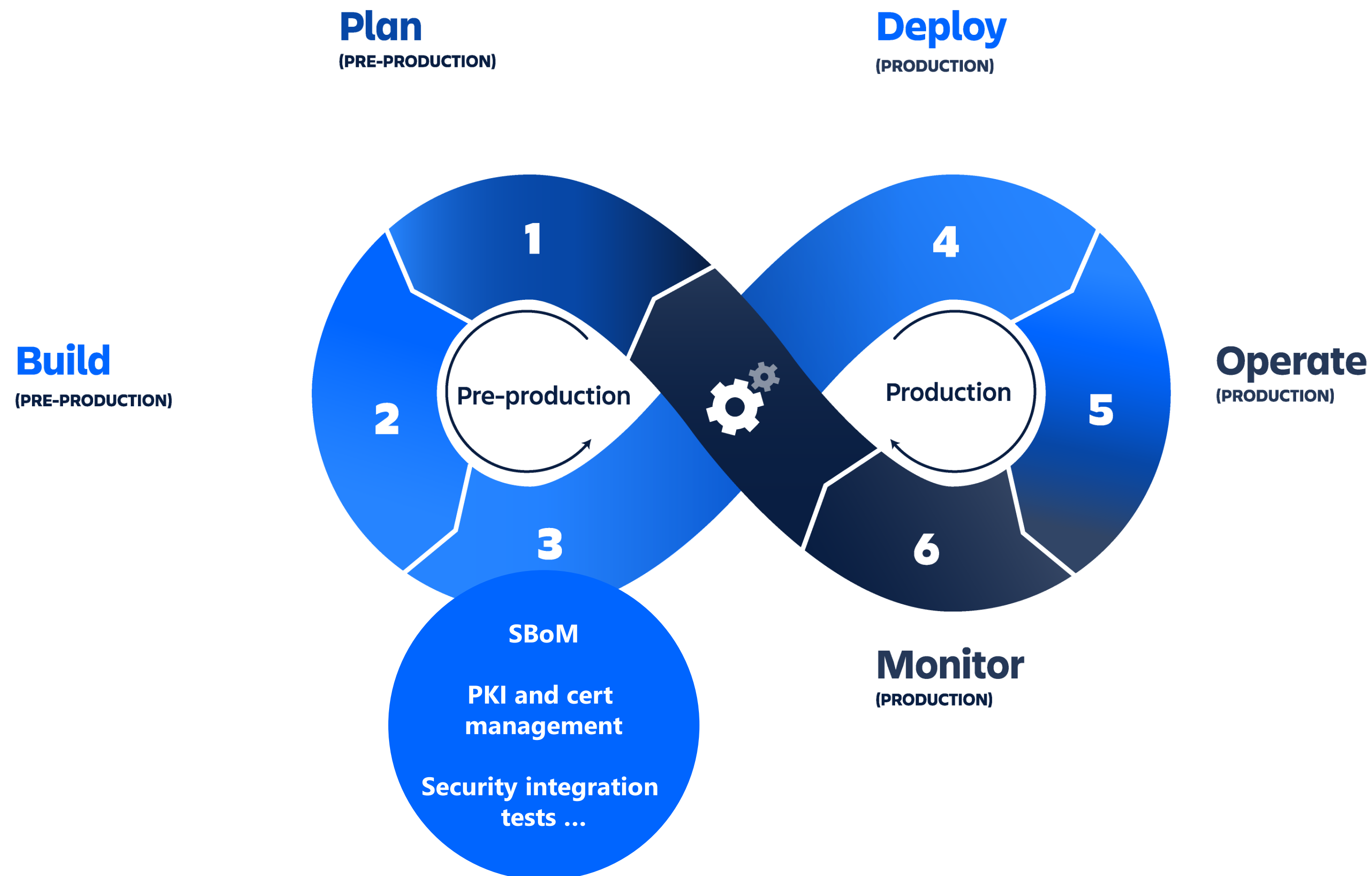


Security is the first concern of every enterprise

Bring together preventive and runtime security models

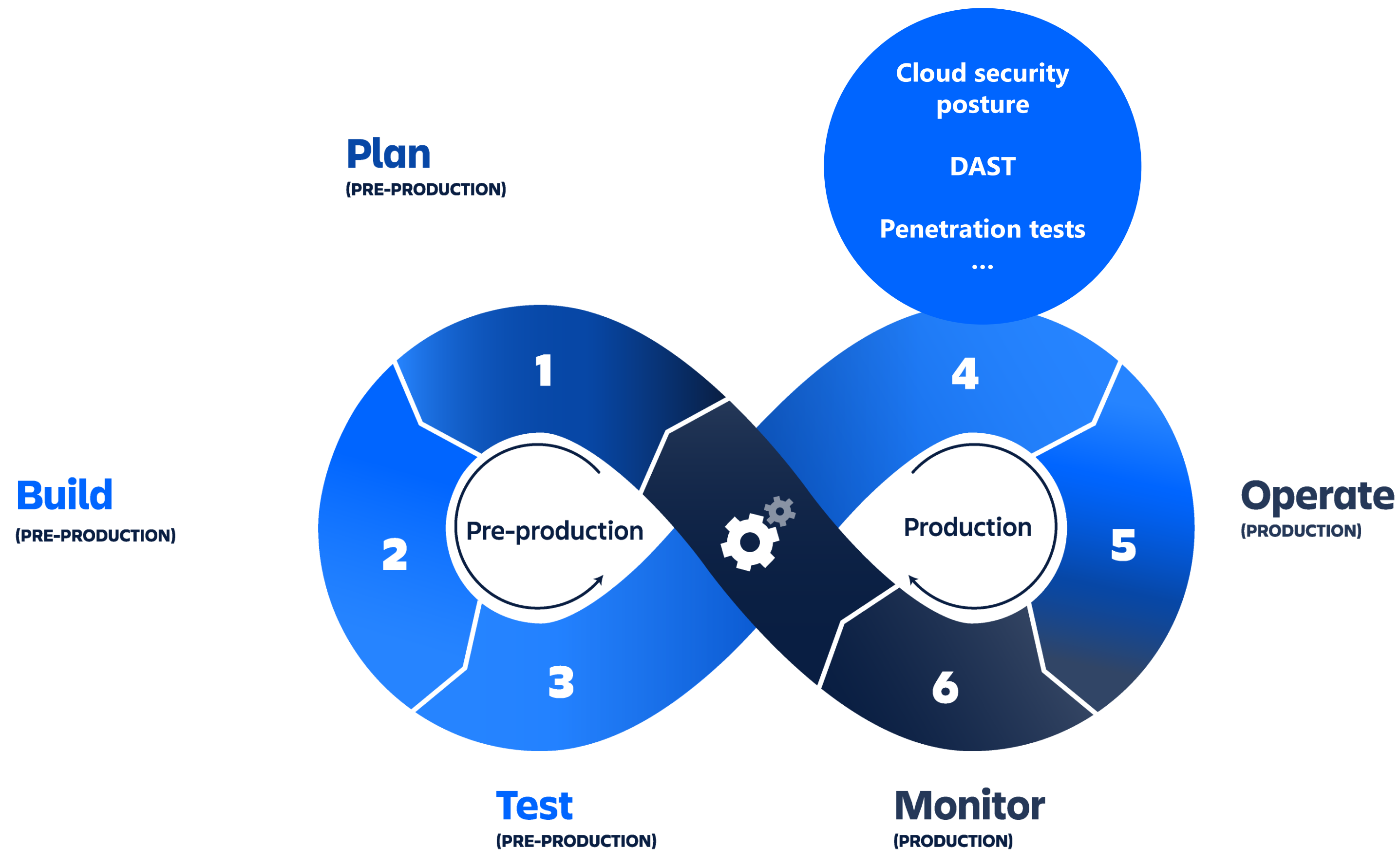


Security is the first concern of every enterprise



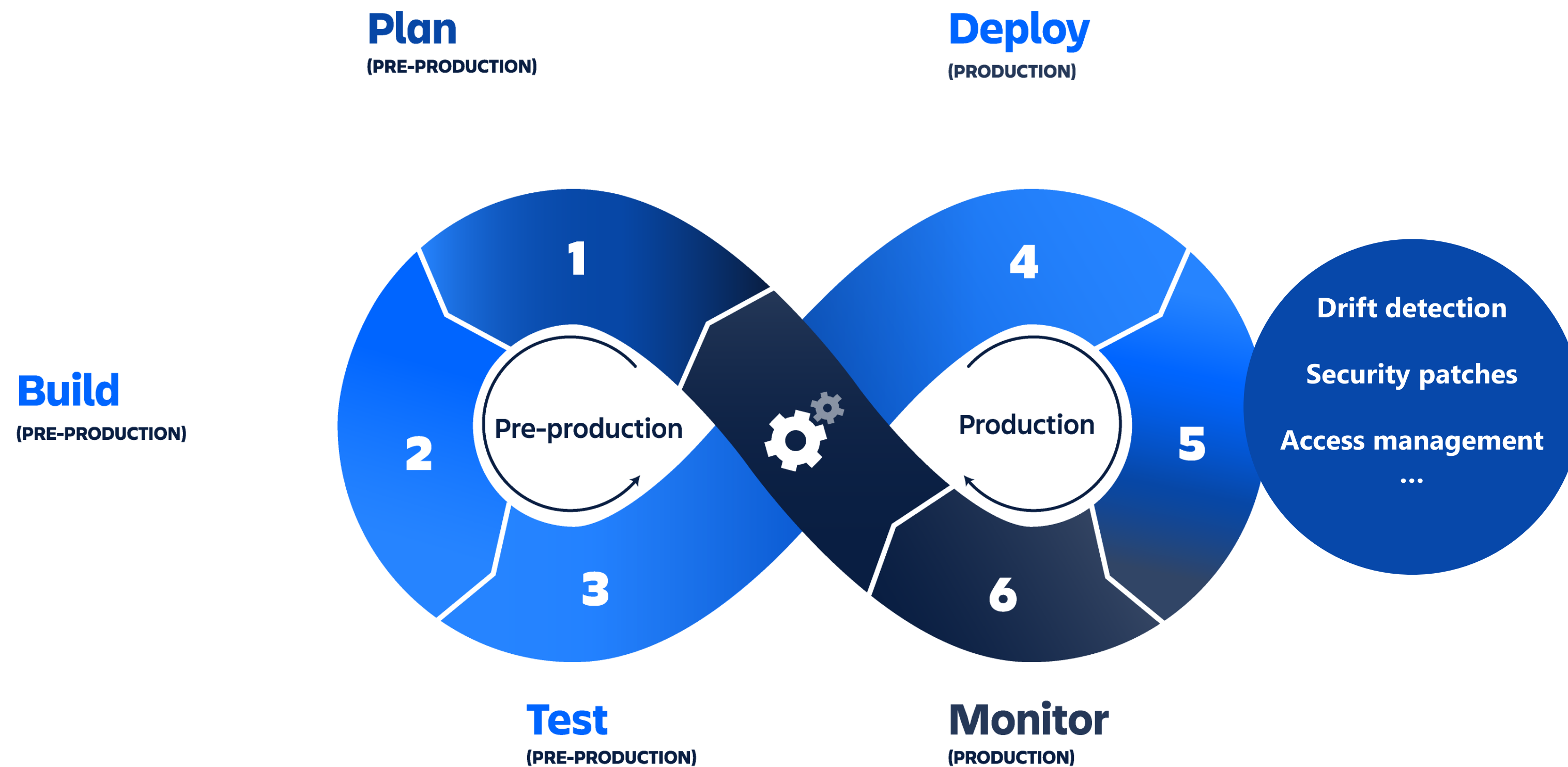
Security is the first concern of every enterprise

Bring together preventive and runtime security models



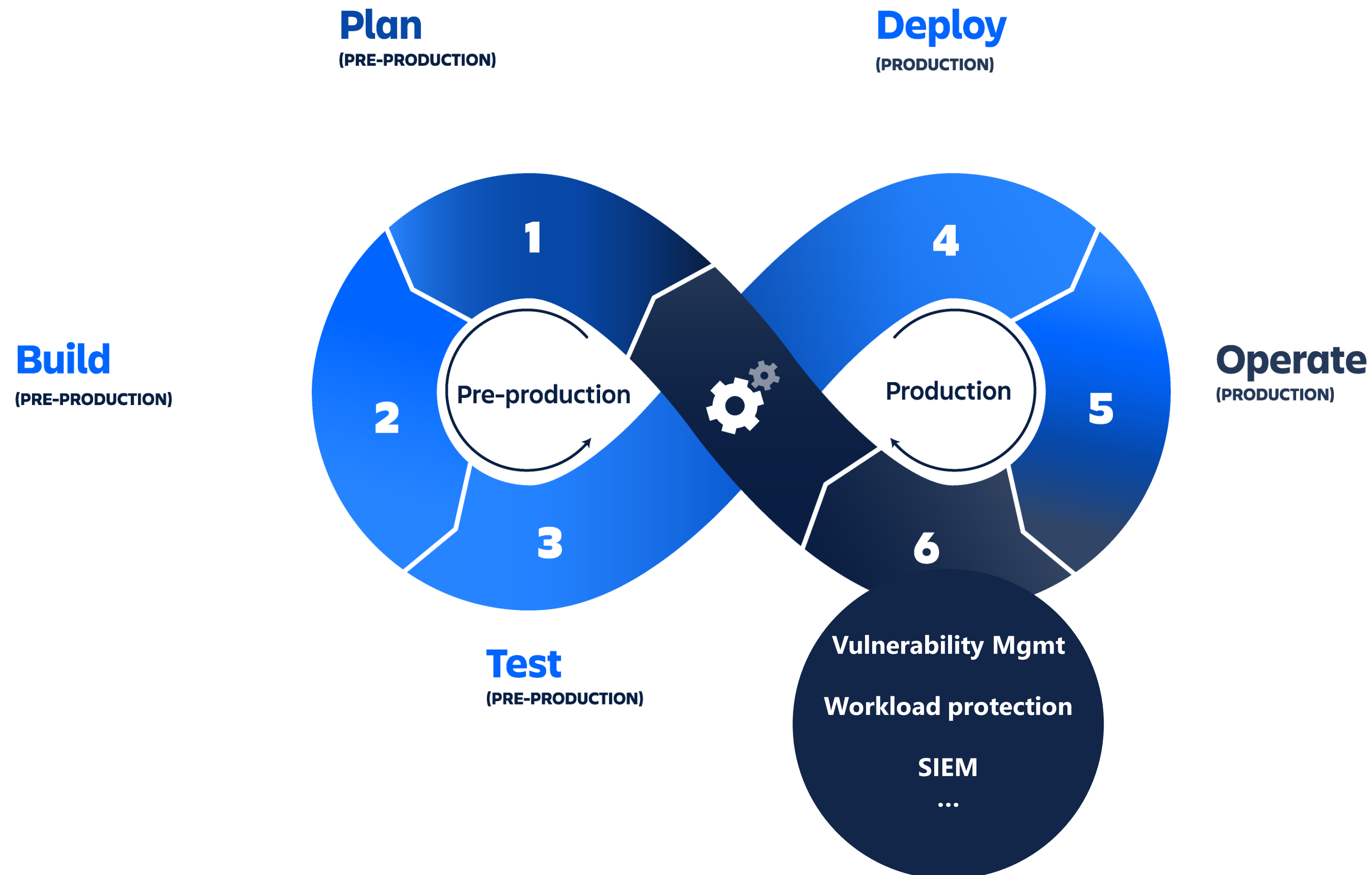
Security is the first concern of every enterprise

Bring together preventive and runtime security models

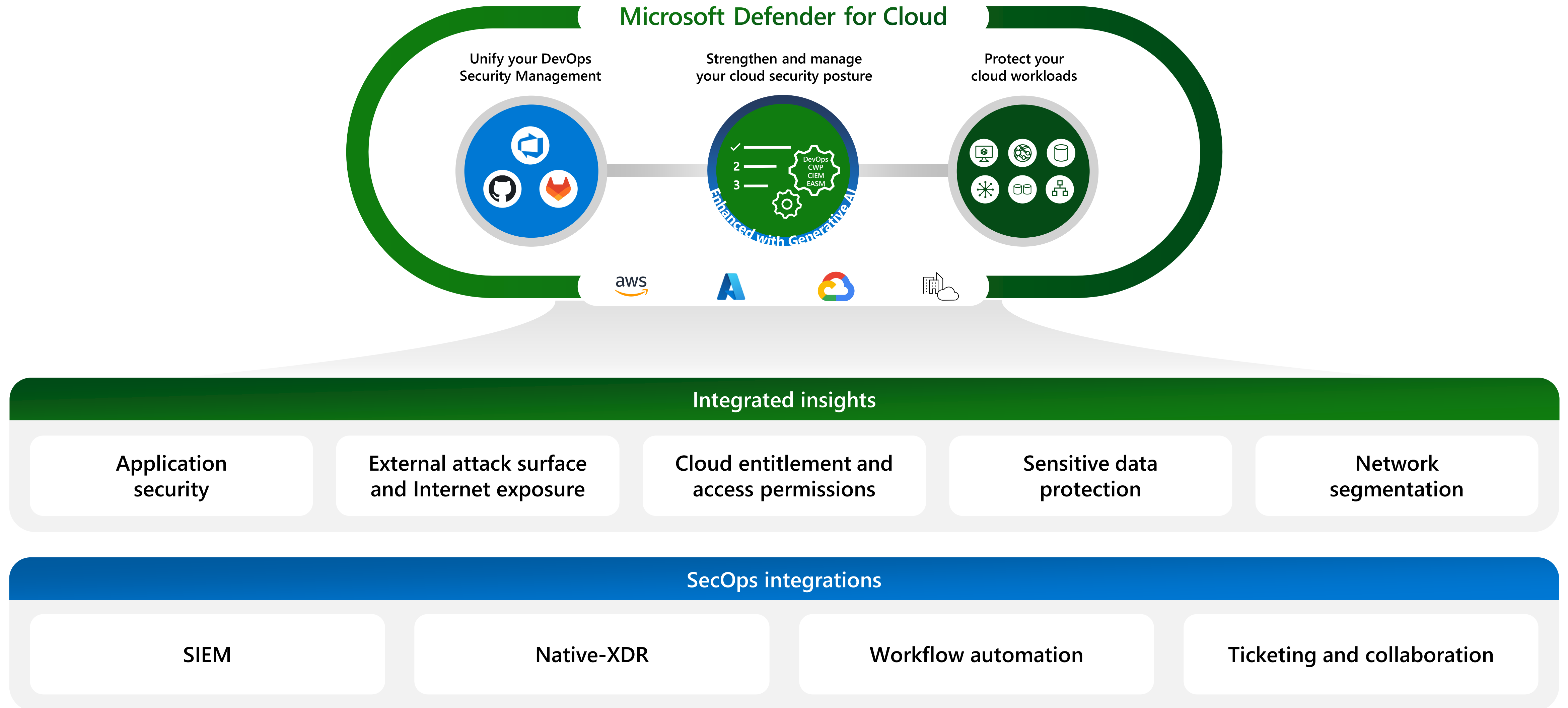


Security is the first concern of every enterprise

Bring together preventive and runtime security models



Access CNAPP capabilities in Microsoft Defender for Cloud



Microsoft approach to API runtime security

Discovery

- Discover the APIs, classify and understand their security posture.

Protection

- Controls put in place based on best practices. Harden API configuration.

Detection

- Analysing API calls for suspicious behaviour

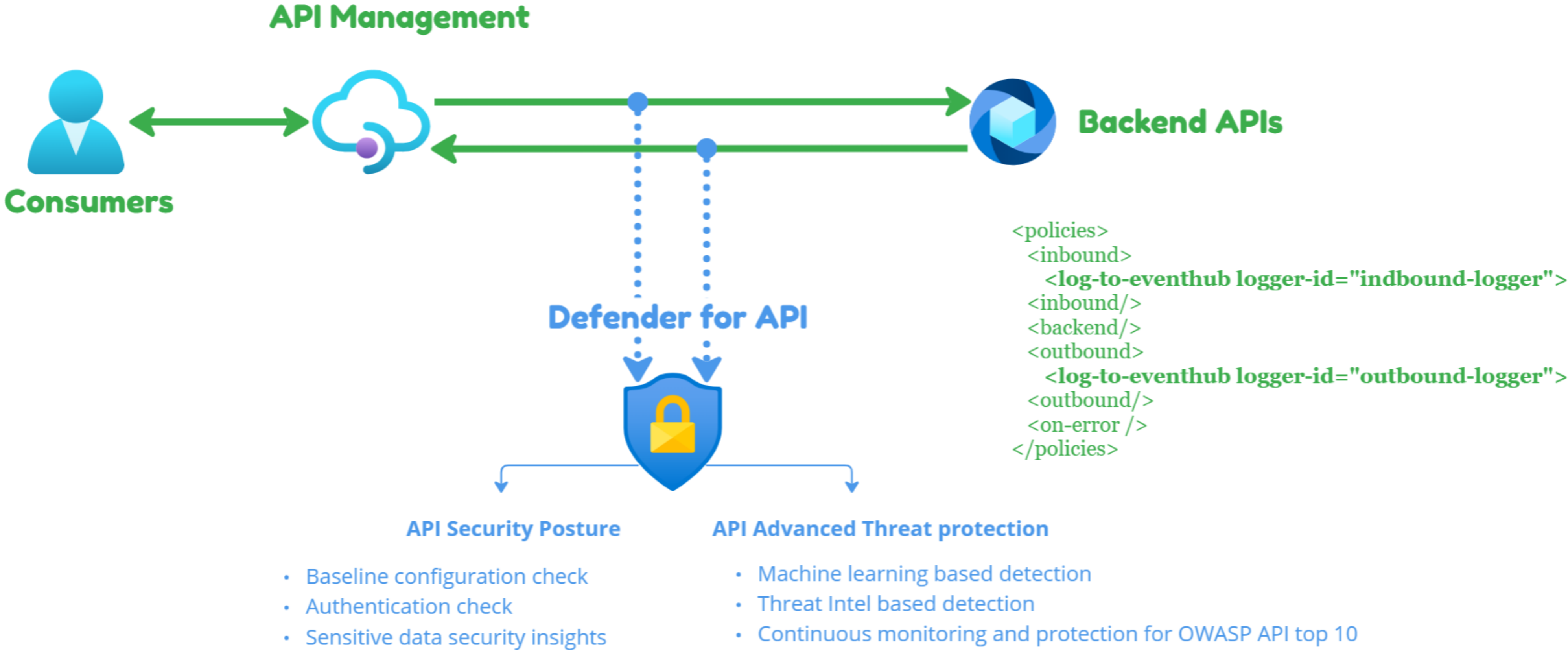
Response

- Recommends remediations methods for vulnerabilities found.

Defender for APIs : Azure API Management integration

Defender for APIs : how does it work?

Transparently mirror traffic to Defender backend



Defender for APIs : how to onboard an API?

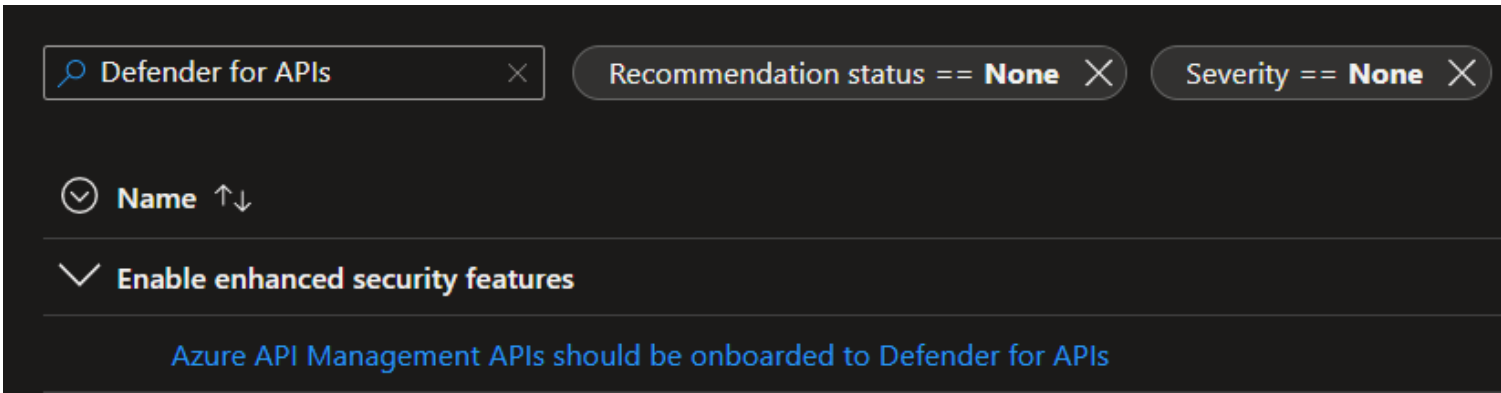
- Enable Defender for APIs

(Defender / Environment Settings / Defender plans)



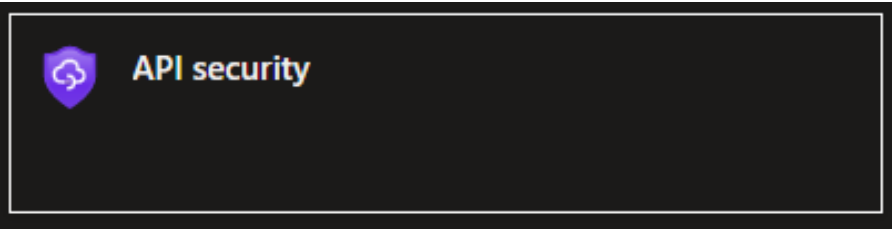
- Onboard an API Management instance

(Defender / Recommendations)



- Analyse

(Defender / Workload Protections / API Security)



Our scenario

4 weeks traffic observation

400M+

Observed traffic

1.21TiB

Data Transfer

60+

Countries

5M

Distinct IP addresses

What did we learn?

Defender for APIs : API security posture

Classify APIs that handle sensitive data and supporting risk prioritization

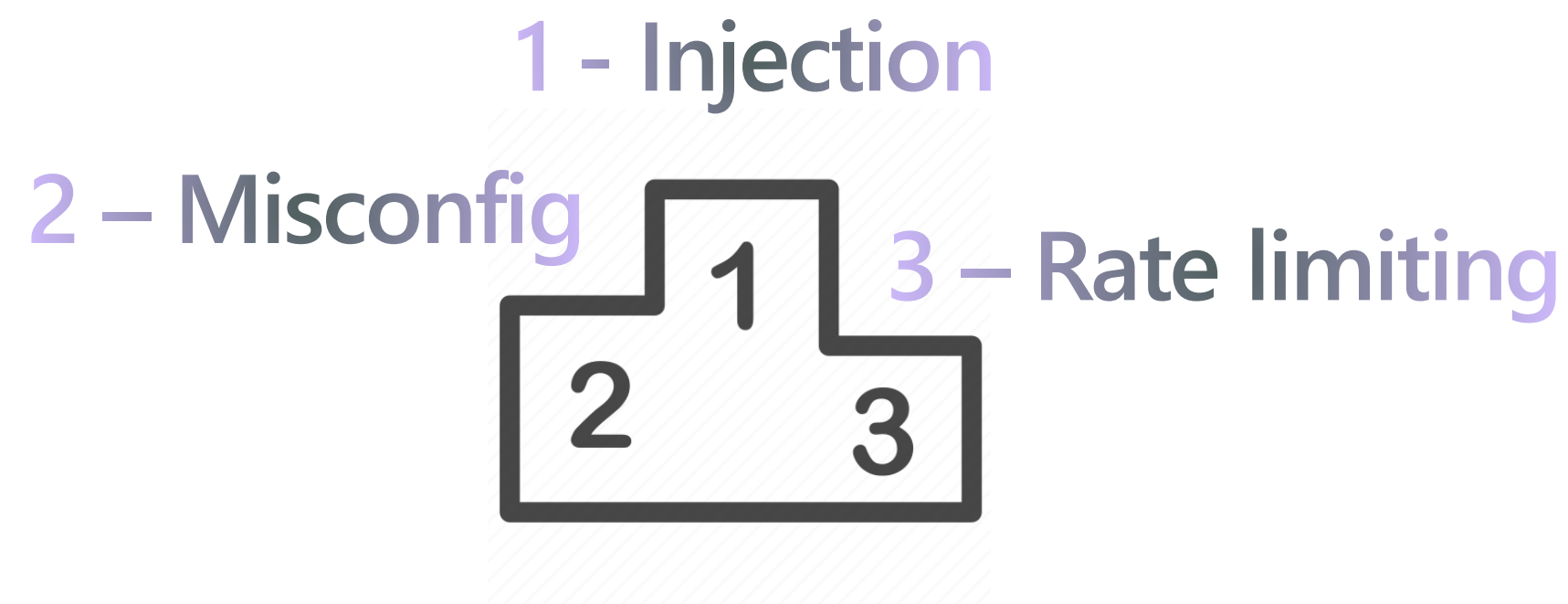
94% of organizations say the most important API security feature is the ability to identify APIs with sensitive data¹

30 Days unused ↑↓	Authentication ↑↓	External traffic observed date (UTC) ↑↓	Data classifications ↑↓
✔ Active	✔ Authenticated		Azure Storage Account Key (Generic)
✔ Active	✔ Authenticated		EU National Identification Number
✔ Active	✔ Authenticated		International Banking Account Number (IBAN)
Awaiting data	Awaiting data	Awaiting data	
Awaiting data	Awaiting data	Awaiting data	
✔ Active	✔ Authenticated		

Defender for APIs : API security posture

Harden API configurations and assess APIM gateway for security best practice controls

23% The second most common OWASP TOP 10 API attack is
#7 Security Misconfiguration¹



API Management security assessment :

- APIM minimum version
- Named value integration with KeyVault
- Check whether the certificate validation follow best practices.
- Avoid all-scope subscription keys.
- Backend authentication
- ... more

Defender for APIs : Advanced threat protection scenarios

- Detect spike in API requests to a single endpoint



OWASP TOP 10 API Targeted vulnerabilities:

- Lack of rate limiting
- Broken user level authentication

Historical Behavior

In the past 30 days, the aggregate user population (all IPs) made an average (mean) of 71.17 API calls to PUT

with a status code of 2XX across 20 minute time windows. Across 20 minute periods, the standard deviation for the number of API calls was 57.8.

[See less](#)

Deviation from Historical Behavior

The event of interest (865 API calls with status code of 2X.

[See more](#)

Security alert

Suspicious population-level spike in API traffic to an API endpoint

Medium Severity | Active Status | 10:10 AM - 11:10 AM Activity time

Alert description

Suspicious spike in API traffic was detected at one of the API endpoints. The detection system used historical traffic patterns to establish a baseline outline API traffic volume between all IPs and the endpoint, with the baseline being specific to API traffic for each status code (such as 200 or 2XX). The detection system flagged an unusual deviation from this baseline leading to the detection of suspicious activity.

Related resource

- API Endpoint
- Subscription

MITRE ATT&CK® tactics

- Impact

Alert details

Take action

General information

Detection Team: Cloud Application Security (CAS)

ResourceId: /Microsoft.ApiManagement/service/

SubscriptionId:

Event of Interest (Spike)

The aggregate user population (all IPs) made 865 API calls to PUT https:// with status code of 2XX in a 20 minute time window.

Historical Behavior

In the past 30 days, the aggregate user population (all IPs) made an average (mean) of 71.17 API calls to PUT with a status code of 2XX across 20 minute time windows. Across 20 minute periods, the standard deviation for the number of API calls was 57.8.

Observed Status Codes

204

Spike (Number of API calls in 20 minutes)

865

Potential causes

This represents a "spike" in API traffic that may indicate a...

Detected by

Microsoft

Deviation from Historical Behavior

The event of interest (865 API calls with status code of 2X...

Actor

Aggregate User Population (All IPs)

Api Endpoint

PUT

Related entities

Azure resource (2)

Azure Developers | APIs in Action

Defender for APIs : Advanced threat protection scenarios

- Users enumerate through API's parameters to expose sensitive information



OWASP TOP 10 API Targeted vulnerabilities:

- Broken object level authentication

Event of Interest
The aggregate user population (all IPs) recently called GET [redacted] and used an average 19563.0 distinct values for parameter [redacted] across several requests in a 20 minute time-window
[See less](#)

Historical Behavior
In the past 30 days, the aggregate user population (all IPs) called GET [redacted] and used an average (mean) of 1075.11 distinct values for parameter [redacted] across 20 minute time windows. Across 20 minute periods, the standard deviation for the distinct number of values used for parameter [redacted] was 1009.96.
[See less](#)

Security alert ⚙ ...

Distributed parameter enumeration on an API endpoint

Medium Severity **Active** Status 10 Activity time 10 PM - PM

Alert description [Copy alert JSON](#)

The aggregate user population (all IPs) was observed enumerating parameters when accessing one of the API endpoints. Based on historical traffic patterns from the last 30 days, Defender for APIs learns a baseline that represents the typical number of distinct parameter values used by the user population (all IPs) when accessing an endpoint in 20-minute windows. The alert was triggered because the user population recently accessed an endpoint using an unusually large number of distinct parameter values.

Related resource

- API Endpoint [redacted]
- Subscription [redacted]

MITRE ATT&CK® tactics ⓘ

- Initial Access

Timeline: [redacted]

Alert details Take action

General information

Detection Team
Cloud Application Security (CAS)

SubscriptionId
f2f58a3e-3bd8-48ae-9592-b41d4f0a5778

Url
[See more](#)

Actor (Client IP)
Aggregate User Population (All IPs)

Parameter of Interest
[redacted]
[See more](#)

Api Endpoint
[redacted]
[See more](#)

Event of Interest
The aggregate user population (all IPs) recently called GET [redacted] and used an average 19563.0 distinct values for parameter [redacted] across several requests in a 20 minute time-window
[See less](#)

Potential causes
This event may represent an attacker exploiting broken o...
[See more](#)

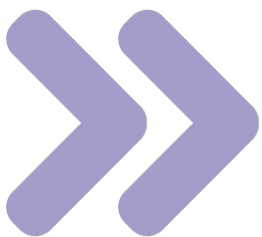
Detected by
Microsoft

Historical Behavior
In the past 30 days, the aggregate user population (all IPs) called GET [redacted] and used an average (mean) of 1075.11 distinct values for parameter [redacted] across 20 minute time windows. Across 20 minute periods, the standard deviation for the distinct number of values used for parameter [redacted] was 1009.96.
[See less](#)


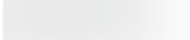
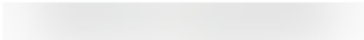
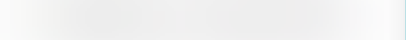

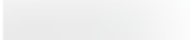
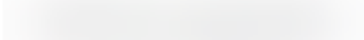
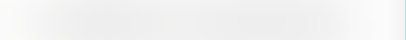

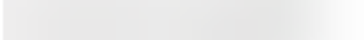
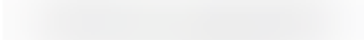
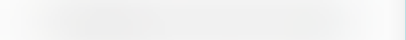

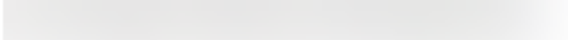
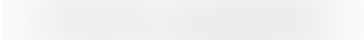
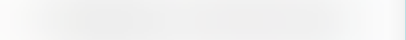
Deviation from Historical Behavior
The event of interest (API calls using 19563.0 distinct values for parameter "[redacted]") is several standard deviations higher than the observed mean.
[See less](#)

Defender for APIs : Microsoft threat intelligence

- IPs that Microsoft threat intelligence has associated with suspicious activities



- OWASP TOP 10 API Targeted vulnerabilities:
- Lack of rate limiting

<input type="checkbox"/> Severity ↑↓	Alert name ↑↓	Affected resource ↑↓	Resource Group ↑↓	Activity start time (UTC)
<input type="checkbox"/> High	API Endpoint access from suspicious IP	 		
<input type="checkbox"/> High	API Endpoint access from suspicious IP	 		
<input type="checkbox"/> High	API Endpoint access from suspicious IP	 		
<input type="checkbox"/> High	API Endpoint access from suspicious IP	 		

Security alert

Suspicious spike in API traffic from a single IP address to an API endpoint

Medium

Active

10:10 PM

Alert description

A suspicious spike in API traffic was detected from a client IP to the API endpoint. The detection system used historical traffic patterns to establish a baseline for routine API traffic volume to the endpoint coming from a specific IP to the endpoint. The detection system flagged an unusual deviation from this baseline leading to the detection of suspicious activity.

Affected resource

API Endpoint

Subscription

Alert details

Take action

General information

Detection Team

Cloud Application Security (CAS)

ResourceId

/providers/Microsoft.ApiManagement/service/

SubscriptionId

Event of Interest (Spike)

Client IP recently made 464 API calls to GET https:// with status code of 2XX in a 20 minute time window.

Historical Behavior

In the past 30 days, distinct IPs accessing GET made an average (mean) of 2.59 API calls to this endpoint with a status code of 2XX across 20 minute time windows.

Deviation from Historical Behavior

The event of interest (464 API calls with status code of 2XX) is several multiples higher than the observed mean for individual users accessing this endpoint.

Actor (Client IP)

Api Endpoint

GET

Observed Status Codes

200

Spike (Number of API calls in 20 minutes)

464

Potential causes

This represents a "spike" in API traffic that may indicate a...

Detected by

Microsoft

Azure Developers | APIs in Action

Defender for APIs : Advanced threat protection scenarios

- Detect spike in API requests to a single endpoint
- Detect unusually large API payload
- Detect parameter enumeration
- Detect spikes by a single identity
- Detect unseen parameters
- Malicious IP Address
- Suspicious User-Agents
- Access from TOR exit node
- ...



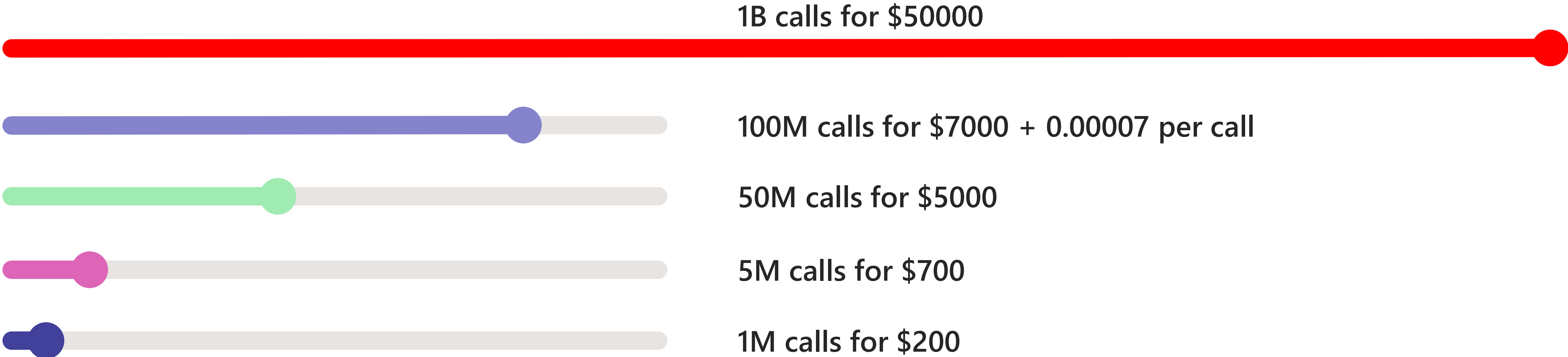
Broken Authentication
Broken Object Level Authorization
Lack of Resource & Rate Limiting
Injection
Excessive Data Exposure
Security Misconfiguration
Improper Inventory Management

...



Defender for APIs : business model

- Pay per pack of APIs + overage (per transaction)



Defender for APIs : GDPR model

Data is retained within the geo boundary. For EU customers, data does not leave the EU boundaries.

- IP addresses are retained for a period of 30 days.
- API request and response bodies are retained for a period of 48 hours (only used for the data classification capability).

The raw HTTP traffic logs are processed by Microsoft backend systems.

- Only resulting metadata (e.g., data classifications, security insights) are displayed to the customer.
- In the case of security alerts, the security alerts themselves will contain the attributed “suspicious” IP address to be used by the customer SOC teams for investigation & remediation.

Defender for APIs does honour GDPR requirements.

- For GDPR DSR Delete requests – No data in-scope for GDPR is retained for longer than 30 days (i.e., all in-scope data already has a max retention for 30 days).
- For GDPR DSR Export requests – Only applicable to in-scope data retained >48 hrs. (i.e., only the IP address).

Thank you