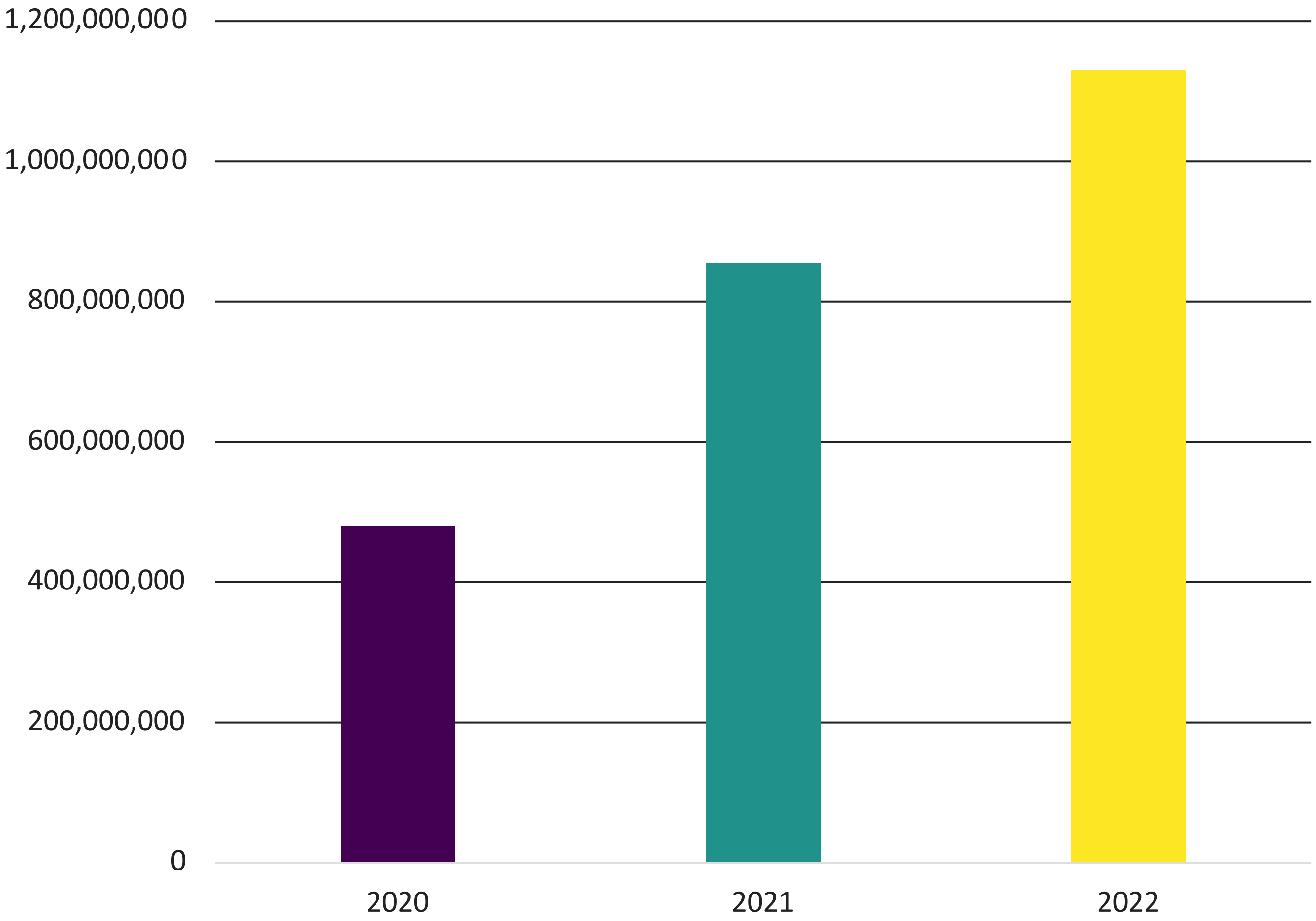
Defense in Depth - API Edition

Shahn Backer | Snr. Solutions Architect | F5

API Growth



Postman

20 M

users

1.13 B

requests made

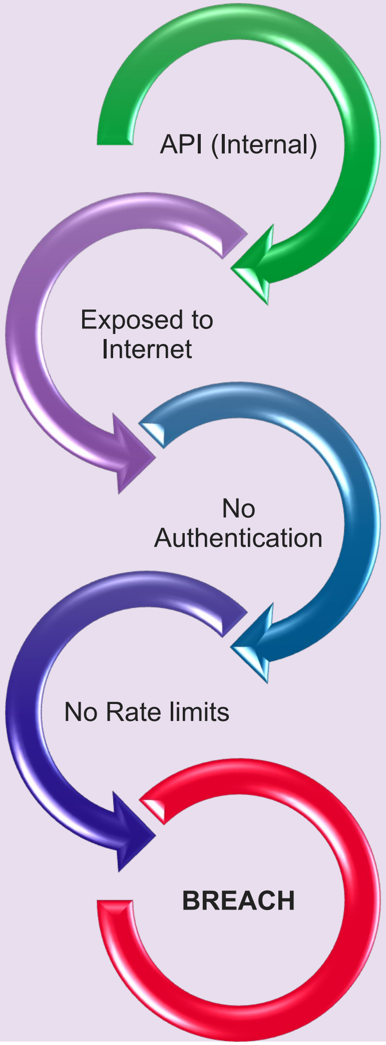
SOURCE: 2022 State of the API Report | Global Growth of APIs (postman.com)

Greater the Growth.. Greater the Attention

Breach Story 1 : Large Telco

- 10 Million customer exposed
- One attacker wanted wanted $1 million in cryptocurrency (Later apologized and claimed to have deleted data)
- Reports suggest breach due to an API available online without authentication

Source: The Guardian



Understand The Exposure
OWASP API Top 10

OWASP API Top 10 (2019)

- API1:2019 Broken Object Level Authorization
- API2:2019 Broken User Authentication
- API3:2019 Excessive Data Exposure
- API4:2019 Lack of Resource & Rate Limiting
- API5:2019 Broken Function Level Authorization
- API6:2019 Mass Assignment
- API7:2019 Security Misconfiguration
- API8:2019 Injection
- API9:2019 Improper Assets Management
- API10:2019 Insufficient Logging and Monitoring

OWASP API Top 10 (2019)

ID	Description	
API1:2019	Broken Object Level Authorization	Identity & Access
API2:2019	Broken User Authentication	Identity & Access
API3:2019	Excessive Data Exposure	Application Security
API4:2019	Lack of Resource & Rate Limiting	Network & Infra
API5:2019	Broken Function Level Authorization	Identity & Access
API6:2019	Mass Assignment	Identity & Access
API7:2019	Security Misconfiguration	Network & Infra
API8:2019	Injection	Application Security
API9:2019	Improper Assets Management	Identity & Access
API10:2019	Insufficient Logging and Monitoring	Application Security

Understanding Security Controls

Reactive vs Proactive vs Predictive

Schools of security controls

	Reactive	Proactive	Predictive
Premise	Time taken by attacker to cause damage is greater than time taken to detect and react	Process and activities performed periodically to identify and eliminate vulnerabilities	Using contextual analysis to identify threats before they become incidents
Examples	Adding IPs to Deny-list after 10 failed logon attempts	Payload inspection by a WAF/WAAP	Behavioral – Malicious user detection
Benefits	Stop-gap when all controls fail	Real runtime protection	Advance warning and protection
Powered By	Logs and telemetry data indicating attacks	Real time analysis of traffic	Machine learning on telemetry data

Types of Controls

Negative vs Positive vs Assistive

Positive Security

1. Allow known good
2. Enforcing Swagger
   - HTTP VERB/Method
   - URL Endpoint
3. Allow API and non-API traffic on the same base URL

Negative Security

1. Rate limiting
2. Malicious Payload check
3. Ip intelligence

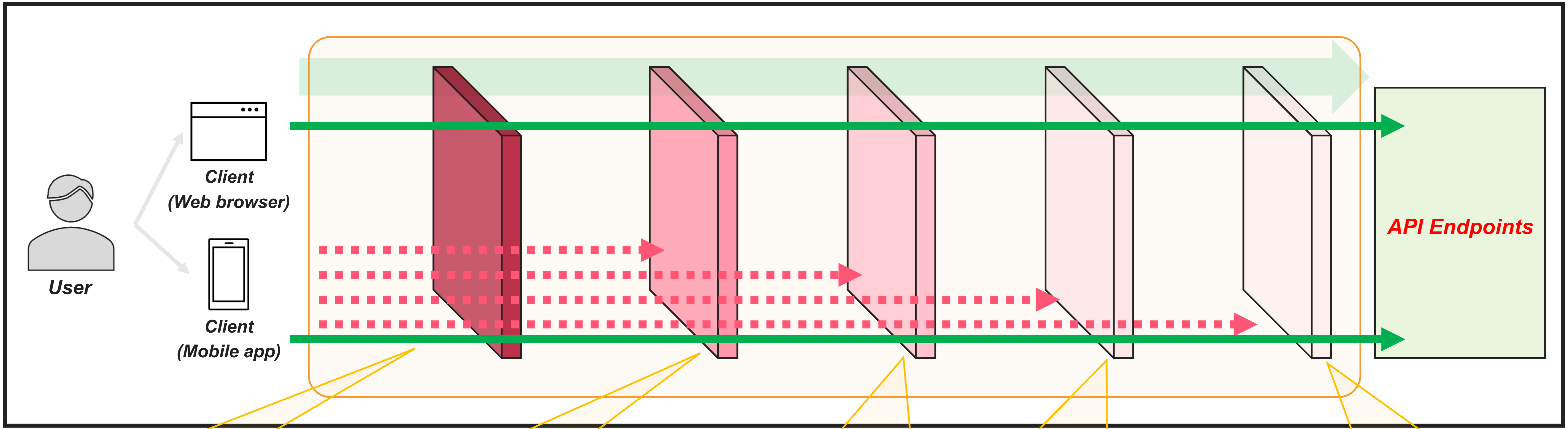
Assistive (Machine Learning/AI)

1. API Discovery
2. Anomaly detection

Defense in Depth for APIs

Defense-in-Depth for APIs

SECURITY AND VISIBILITY THAT COUNTS



Perimeter defense

- DDoS protection
- Rate-limiting
- Bot defense

Network defense

- SSL Decryption
- Intrusion Prevention
- Firewall monitoring

Application defense

- WAAP
- Anomaly detection
- Shadow API discovery

Data defense

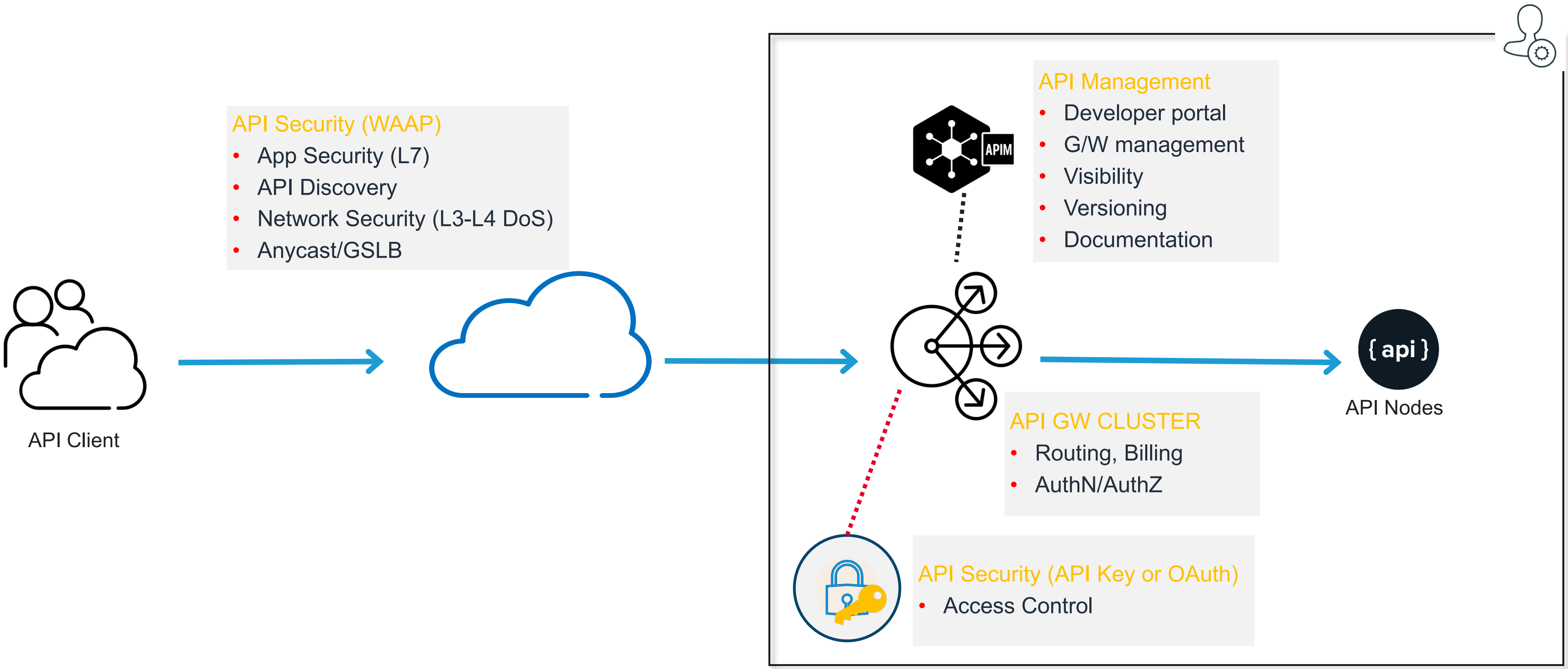
- Modern authentication
- Advanced access control
- Sensitive data masking

Policy and Procedures

- Risk management
- Audit and monitoring

Deploying the Controls

Deploying Security Controls for API



API Security (WAAP)
- App Security (L7)
- API Discovery
- Network Security (L3-L4 DoS)
- Anycast/GSLB

API Management
- Developer portal
- G/W management
- Visibility
- Versioning
- Documentation

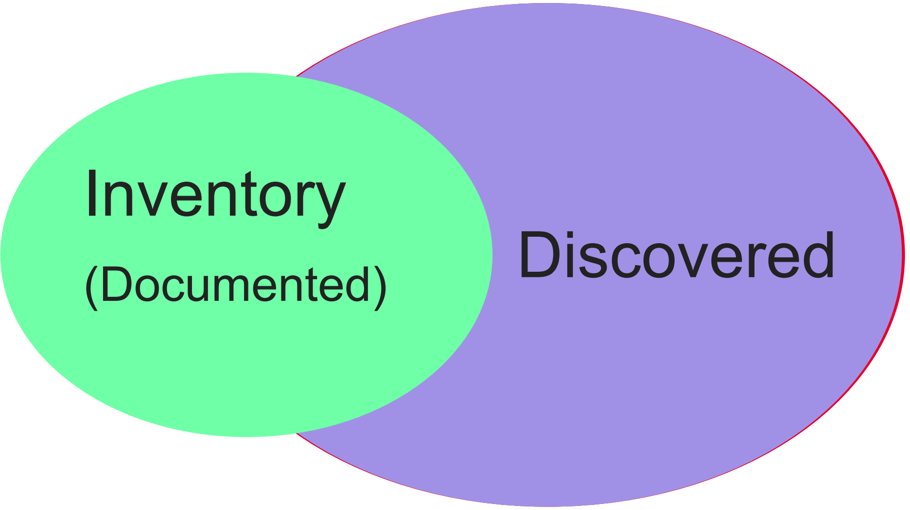
API GW CLUSTER
- Routing, Billing
- AuthN/AuthZ

API Security (API Key or OAuth)
- Access Control

Demo

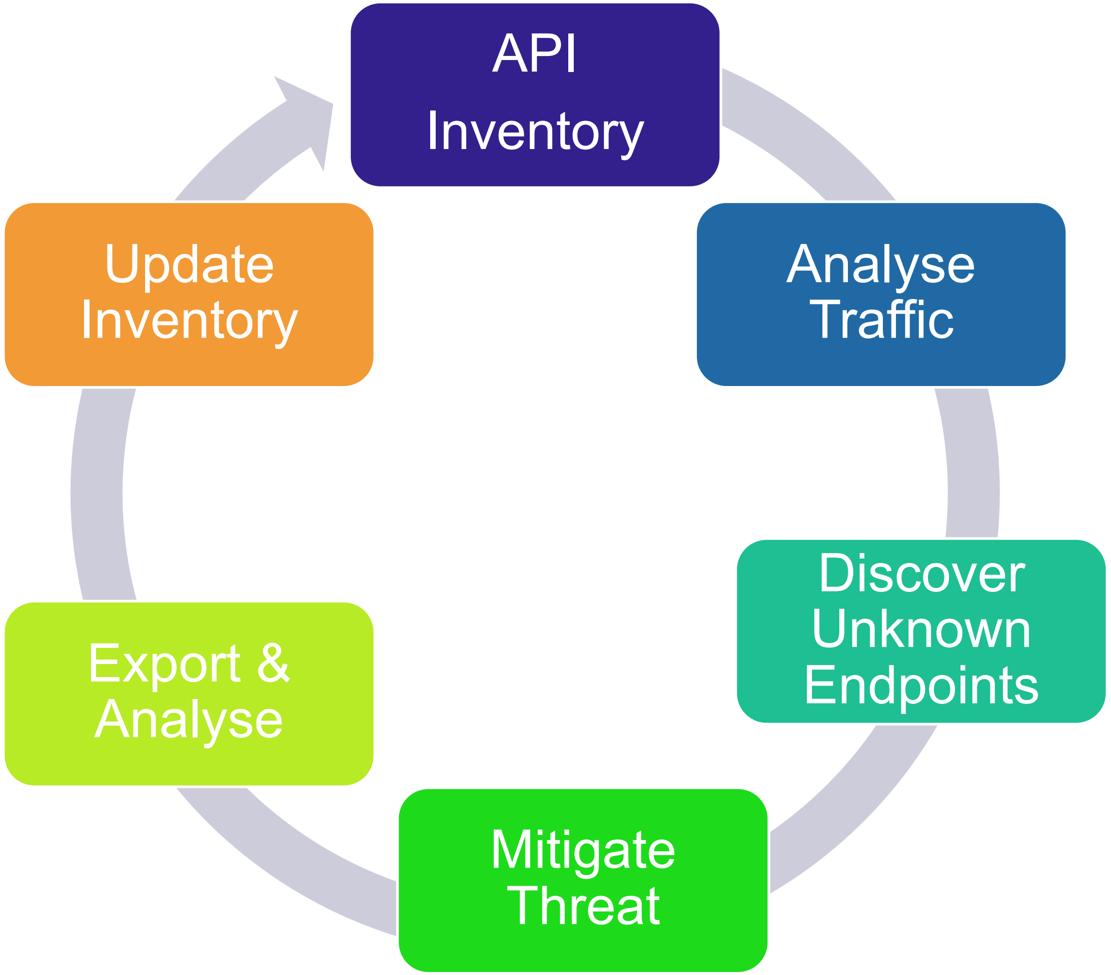
Shadow APIs Detection and Mitigation

Shadow APIs & How to tackle them

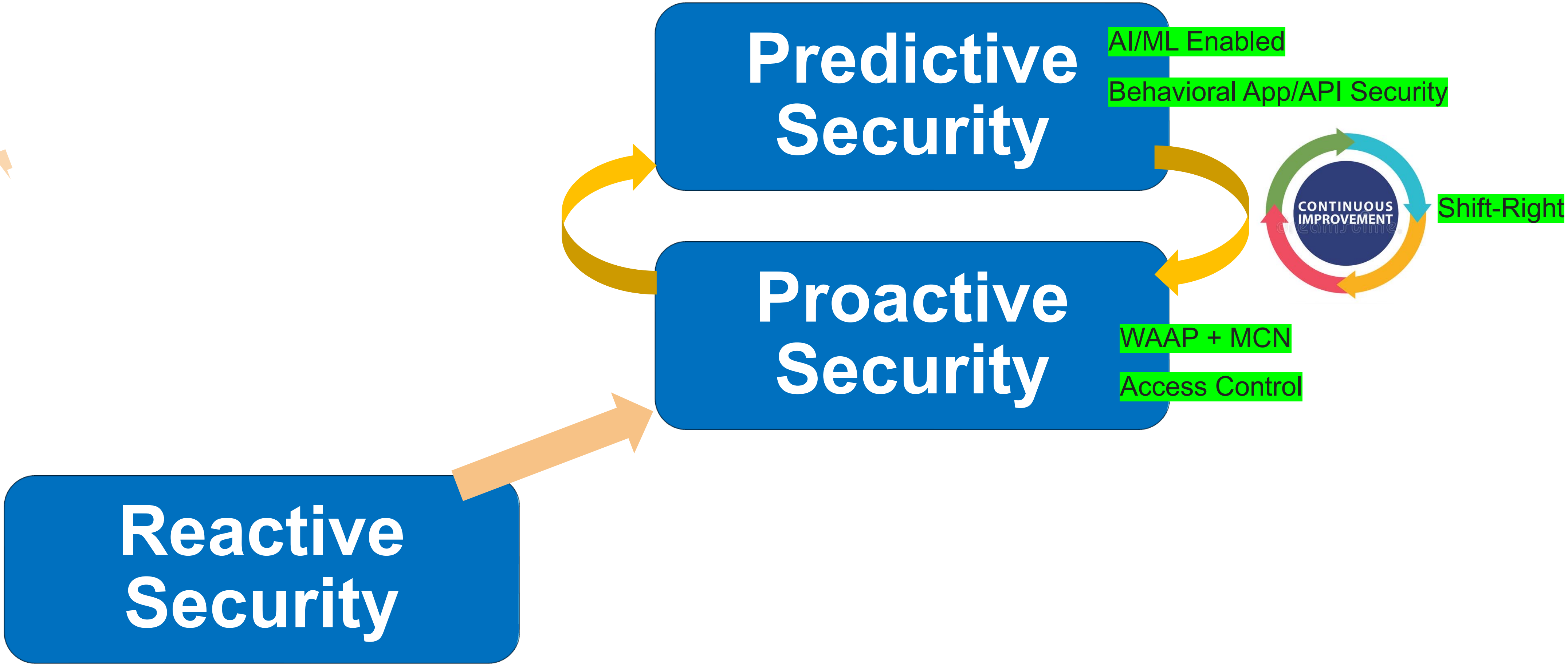


Threat mitigation techniques

- Allow/Deny request
- Rate Limits



API Security Maturity Model at Runtime



Predictive Security

AI/ML Enabled

Behavioral App/API Security

Shift-Right

Proactive Security

WAAP + MCN

Access Control

Reactive Security