QSC24

Manage the Attack Surface of Your APIs

Kunal Modasiya
Vice President, Product Management
Attack Surface Management, Web App & API Security
Cloud & Container Security
April 24

Agenda

01 Use Cases

02 Learnings from Design Partners

03 Comprehensive Discovery

04 Roadmap

API Security Use Cases

Discovery & Inventory

- Identify all APIs in your environment, including **internal**, **external**, **rogue** and **shadow** APIs
- Categorize APIs based on their sensitivity, usage, and **potential attack surface**
- Focus security efforts on high-risk APIs first

Compliance & Conformance

- OpenAPI Specification v3 (**OAS**)
- Active & passive compliance for **Swagger**
- 200> detections

Vulnerability Testing

- **OWASP API Security Top 10**
- **PII** & **Sensitive** Data detections
- Continuous addition of API detections for increased coverage
- **200> detections**

Prioritization & Remediation

- **Prioritize** identified vulnerabilities based on severity, potential impact, and exploitability
- Utilize **"TruRisk"** to help prioritize APIs across the organization
- Address **critical vulnerabilities** first to mitigate the most significant **risks** to your organization

Shift-Left & Shift-Right

- Building a **"Shift Left"** & **"Shift Right"** proactive security policy is a must have for modern development and **security practices**.
- Streamlining the **CI/CD** pipelines and **incident management** workflows with automation is vital

Qualys.

Design Partner Interest

AMERICAS

CISA
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

HCA Healthcare

TD Bank
America's Mc

NVIDIA

SONY MUSIC

FCC Federal Communications Commission

Honeywell

EMEA

AXA

RBS
The Royal Bank of Scotland

TESCO

BAT

JM Johnson Matthey
Inspiring science, enhancing life

eDF

UH Geneva Medical Center

centrica

KPMG

APAC

Telstra

Standard Chartered

AustralianSuper

Australian Unity
Real Wellbeing

Digital Labs

EY
Building a better working world

Key Learnings from Design Partners

API attack surface Discovery is most critical

Unified Risk View of Web Apps and APIs is important

Have separate project and Budget Part of AppSec

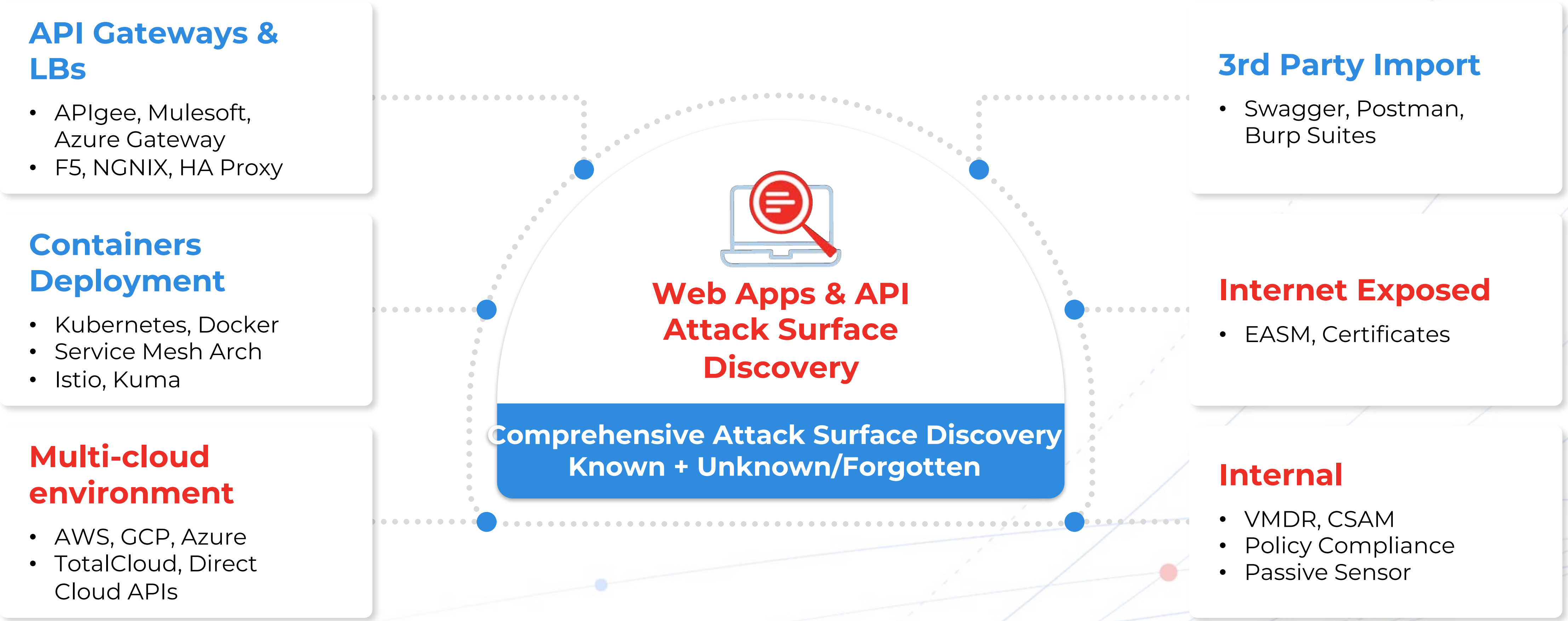
Most Organizations are looking to Kick-off API Security Testing Initiative

Attack Surface Discovery : Web Apps and API

Qualys.

Attack Surface Discovery Strategy

Web Apps and APIs



API Gateways & LBs

- APIgee, Mulesoft, Azure Gateway
- F5, NGNIX, HA Proxy

Containers Deployment

- Kubernetes, Docker
- Service Mesh Arch
- Istio, Kuma

Multi-cloud environment

- AWS, GCP, Azure
- TotalCloud, Direct Cloud APIs

Web Apps & API Attack Surface Discovery

Comprehensive Attack Surface Discovery
Known + Unknown/Forgotten

3rd Party Import

- Swagger, Postman, Burp Suites

Internet Exposed

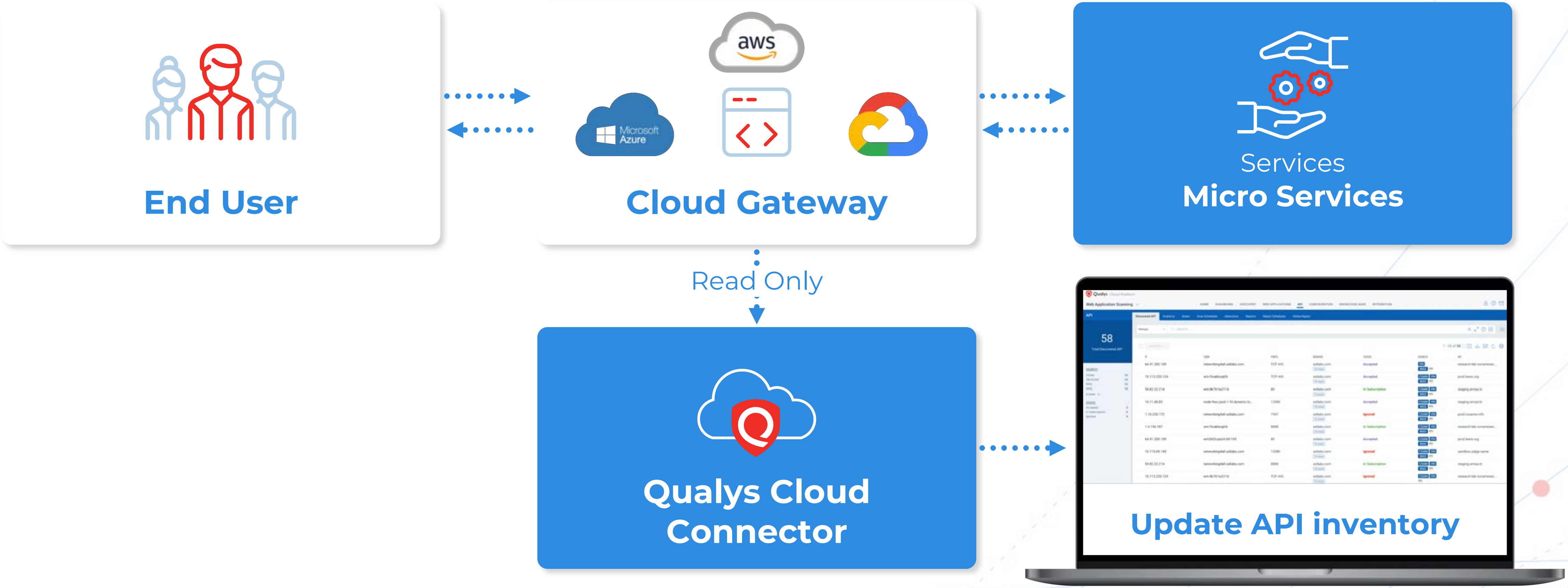
- EASM, Certificates

Internal

- VMDR, CSAM
- Policy Compliance
- Passive Sensor

Qualys.

Cloud API Discovery



End User

Cloud Gateway

Services
Micro Services

Read Only

Qualys Cloud Connector

Update API inventory

API based connector to read configuration and populate inventory

Roadmap

Qualys.

Multi-Phase Roadmap for AppSec Security

Q2 2024

WAS

- WAS and API Detection Enhancements
- Customer FRs, New UI, Scanner Roll out
- Certificate Inventory for web apps
- Webapp Discovery from TotalCloud
- WAS Free Report

API Security

- Inventory – Swagger, Postman API Collection import - REST and SOAP APIs
- API Vuln Testing (OWASP API TOP 10) - 7/10 support
- API Compliance (API documentation to OAS v3)
  - Additional 135 detections
- TruRisk Score based Prioritization for APIs

2H 2024

WAS

- Customer FRs, New UI parity
- VMDR Integration - Discovery of web application from VMDR (Q3 24)
- CSAM CMDB – Integrate all assets part of Application and TruRisk Reporting for App

API Security

- Shift left integration with Jenkins, Azure
- Ticketing Integration with ServiceNow
- Discovery of APIs
  - Integration with AWS, Azure & GCP Cloud
  - Integration with API gateways – APIGee, Azure Gateway
  - EASM discovery of public API end points
  - API Discovery from webapp scans

Sign Up for Beta Trial – May 2024

*Roadmap may be subject to change

Qualys.® | De-risk Your Business