Managed Application Security Testing

Frictionless application security testing

Application Security (AppSec) programs are becoming more complex, often keeping organizations preoccupied with daily operations and preventing them from focusing on strategic initiatives. KPMG Managed Application Security Testing allows organizations to leverage a trusted third party to manage the full spectrum of AppSec testing, from strategic enhancements to day-to-day operations.

1 Web App exploits are still the most common form of attack

2 Developers are tasked to innovate faster adding complexity

3 Security is not equipped to keep up with acceleration of development

4 Time to remediate can take up to 6 months for most businesses

Application and API Pen Testing
KPMG streamlines manual penetration testing to regularly test for configuration vulnerabilities.

Dynamic Application Testing
KPMG facilitates scheduled DAST scans to test for runtime vulnerabilities in the application.

SAST and SCA
KPMG leverages Software Composition Analysis (SCA) and Static Application Security (SAST) scans to test application dependencies and static code for vulnerabilities.

Code and architecture review
Manual review informed by SAST and SCA results, and design review focusing on logical placement and dependencies.

| AppSec at DevOps speed | Scan orchestration | Analyst-driven service | Centralized reporting | Predictable cost |

KPMG removes complexity

Enterprises typically require different testing types for large application portfolios. Our process is designed for a frictionless experience:
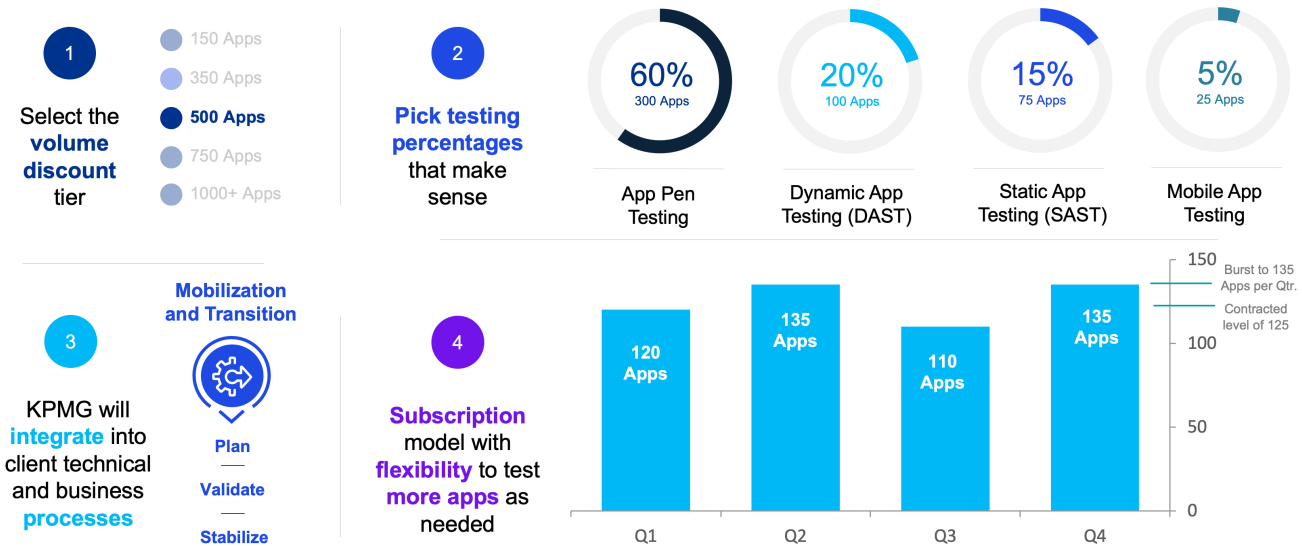
- Define total number of applications

- Pick the required testing types each app

- Decide on testing percentages that make sense

KPMG will provide flexibility on app size and give you room to grow your overall app portfolio.

Service is based on a subscription model that allows for predictable costs and testing frequency. Additional services include:

- Security questionnaire review

- Basic application architecture review

- Monthly Ask-Me-Anything (AMA)

- Advanced application architecture review for critical apps

- Volume discounts

Example

1

Select the **volume discount** tier

- 150 Apps
- 350 Apps
- **500 Apps**
- 750 Apps
- 1000+ Apps

2

Pick testing percentages that make sense

60%
300 Apps
App Pen Testing

20%
100 Apps
Dynamic App Testing (DAST)

15%
75 Apps
Static App Testing (SAST)

5%
25 Apps
Mobile App Testing

3

KPMG will **integrate** into client technical and business **processes**

Mobilization and Transition

Plan
—
Validate
—
Stabilize

4

Subscription model with **flexibility** to test **more apps** as needed

120 Apps (Q1)
135 Apps (Q2)
110 Apps (Q3)
135 Apps (Q4)

Burst to 135 Apps per Qtr.
Contracted level of 125

Contact us

Rajesh Ahuja
Managing Director, Cyber Managed Services
T: +1 602 321 8026
E: rajeshahuja@kpmg.com

kpmg.com/socialmedia

Evan Rowell
Director, Managed Application Security Testing
T: +1 704 421 3556
E: erowell@kpmg.com

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.