



Managed Security Testing

Continuous security validation driving measurable risk reduction at enterprise scale



Modern enterprises face growing vulnerability volumes and limited remediation capacity. KPMG Managed Security Testing combines risk-based prioritization, exploit validation, and remediation verification to accelerate closure at enterprise scale.

Are you discovering vulnerabilities continuously, but struggling to prioritize, validate, and close them?

Are remediation SLAs missed due to noisy findings and limited retesting capacity?

Do auditors or regulators expect proof that risk has been validated and resolved, not just identified?

Did you know?



84%

of organizations report an increase in cyber attacks over the past year



56%

of security leaders view AI, GenAI, and Agentic AI as a top emerging security threat

Source: [KPMG 2026 Cybersecurity and Technology Risk Survey](#)

Overall, companies around the world are facing shortages of certified, specialized testers.

Does your security team have the time to test your systems thoroughly and routinely?

Potential benefits



Enterprise-scale asset and application visibility



Risk-based prioritization based on business impact



Reduction of vulnerability remediation backlogs



Governance, SLA tracking, escalation, and reporting



Risk exception and acceptance management



Executive and operational dashboards



Continuous validation of remediation effectiveness



Trend analysis and security program maturity improvement

KPMG Managed Security Testing (MST) enables risk reduction through testing, validation, and advisory capabilities. MST combines enterprise vulnerability management, scalable security testing, governance, and continuous validation, designed to discover, prioritize, validate, track, and confirm closure of risk across the enterprise.

MST helps organizations move beyond scan results to managed risk reduction.

MST combines automated discovery, AI-enabled testing, exploit validation, governance, and remediation verification, aimed at accelerating security testing, improving coverage, and validating remediation effectiveness. The result is a scalable, defensible vulnerability management program that can reduce remediation backlogs, improve SLA performance, and strengthen security maturity over time.

Why KPMG MST

Deep experience operating enterprise vulnerability management and testing programs **at scale**

Integration of vulnerability management, scalable security testing, governance, and continuous validation

Broad coverage across apps, APIs, infrastructure, cloud, and AI-enabled environments

Consistent delivery, quality, governance and reporting model

Market-tested ability to reduce vulnerability backlogs and validate remediation effectiveness

Cost stability

Avoid annual rate increases with a multi-year agreement, creating predictable spend and long-term savings for the duration of the engagement.



KPMG Managed Security Testing



Lower cost per test

Clients typically benefit from reduced per-test pricing driven by long-term planning, resource optimization, and guaranteed annual spend.

Continuous relationship

Get more frequent touchpoints and a steady rhythm, better reflecting how real adversaries operate continuously rather than once per year.



Greater flexibility

Shift between different testing types on our menu without additional paperwork or administrative delay.

KPMG Managed Security Testing is built to provide consistent service quality, delivery, governance, and communication cadence to support managed risk reduction. MST can help strengthen your security posture, while enabling confidence as you innovate and protect critical systems.



To learn how you can benefit from KPMG Managed Security Testing, get in touch.



Evan Rowell
Managing Director, Advisory
Cyber Managed Services
KPMG US
erowell@kpmg.com



Wes Cole
Director, Advisory
Cyber Managed Services
KPMG US
westoncole@kpmg.com

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved. KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit kpmg.com/governance.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.