Four Signs It's Time to Expand Your Security Testing

A penetration test reflects a point-in-time environment. As the product, infrastructure, or attack surface evolves, testing scope should evolve with it. If any of the four situations below apply, it's likely time to expand testing.

1

You've shipped new AI features

LLM features, agents, RAG, and MCP servers open attack paths a standard web pentest doesn't cover: prompt injection, insecure tool use, excessive permissions.

Recommend: AI Pentest + targeted threat modeling.

2

You've launched on mobile

iOS and Android apps carry attack surface a web app pentest doesn't reach: local storage, device permissions, certificate validation.

Recommend: Mobile App Pentest, per version.

3

An enterprise prospect wants more coverage

Vendor security reviews often expect testing beyond your original scope: APIs, integrations, admin functionality, authorization, network segmentation, cloud configurations, and source code.

Recommend: Expand scope to match what's being requested.

4

You've been through a merger or acquisition

Consolidation leaves overlapping credentials, identities, and permissions. New products, hybrid and multi-cloud infrastructure, and new team members widen risk across every environment.

Recommend: Internal Network Pentest, Secure Cloud Review, Red Teaming, Social Engineering.

Your product has evolved. Make sure your security testing has too.

These services can be added to your existing engagement.

Scope Your Next Engagement