Partners in defense,
experts in offense

Kaspersky Application Security Assessment

kaspersky bring on the future

Offensive security experts

Leveraging our proven approach grounded in deep expertise and industry standards, our team of experts in practical cybersecurity simulates real-world attack techniques to deliver a bespoke assessment — from complex multi-network infrastructures to individual solutions.

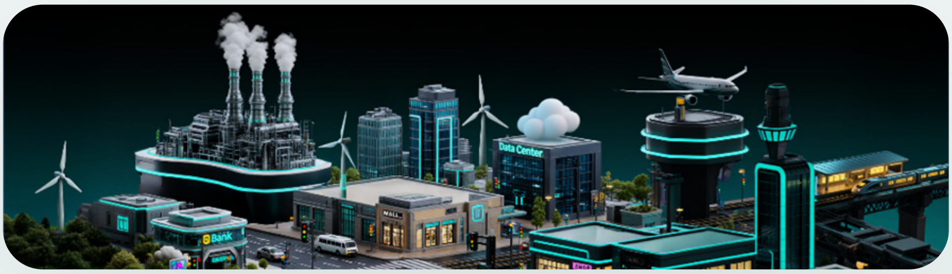
What is application security assessment

Regular application security assessment is foundational for any technology-driven business. Ensuring the security of critical assets is a key factor in maintaining long-term success and operational efficiency.

Service identifies business logic flaws, misconfigurations, and other critical vulnerabilities. We demonstrate their real-world business impact from data breaches to disruption to core services and deliver a clear remediation plan.

How it helps:

- Enhance the security posture of critical assets and improve software development quality
- Translate technical risks into business terms to demonstrate the strategic value of security investments
- Identify and remediate security vulnerabilities, gaps and business logic flaws before adversaries can exploit them and harm your business



Kaspersky Application Security Assessment

Security foundation for business

Key advantages:

Industry insights

Our team provides tailored insights for your unique challenges, backed by hands-on experience in industries

- Power and utilities
- Manufacturing
- Oil and gas
- Transportation
- Banking
- IT

Collaborative intelligence

We collaborate with Kaspersky's Incident Response and Threat Intelligence teams to ensure access to the latest cyber threat data and insights.

Proven research leadership

Our experts regularly publish researches and discovered vulnerabilities (CVEs) in major companies such as Oracle, Google, Apple, and Microsoft.

Kaspersky experts adopt, develop and tailor a customized testing approach for each application and your organization's requirements, following the process below:

1 Preparation

- Information gathering
- Threat model alignment
- Defining testing approach — grey-box or white-box

2 Assessment

- Vulnerability discovery
- Exploitation
- Business logic flaws identification

3 Reporting

- Technical report
- Executive summary

The assessment covers a broad spectrum of systems — corporate and internet-facing applications, mobile and desktop software, as well as integrated hardware-software solutions. Our proven methodology applies to a wide range of systems, including:

- Mobile apps
- Web apps
- Cloud solutions
- API
- Firmware
- Desktop
- E-commerce
- Online banking
- B2B solutions
- Hardware

Key features

Our experts go beyond standard vulnerability scans and OWASP Top 10, conducting in-depth security assessments that exposes logic flaws, misconfigurations, and vulnerabilities of the applications. To achieve this, we employ a comprehensive approach that combines manual security testing, proprietary solutions, and industry-standard automation tools.

Our application security assessment methodology follows industry best practices and includes the following testing approaches:

Grey-Box Testing

- External attacker
- Application user
- User with specific role (e.g., user, admin, partner)

This method simulates a real-world attacker with valid credentials, as defined by the threat model. Grey-box testing does not require access to the source code and closely resembles the scenario of an external attacker with limited system knowledge

White-Box Testing

- Developer
- User with specific knowledge about application
- User with leaked source code

This method is conducted with full access to source code, application architecture, and data flow documentation. This approach applies comprehensive analysis, allowing security experts to uncover deep-rooted vulnerabilities in design, implementation, and configuration

Kaspersky Application Security Assessment

Attacker-driven analysis for real-world defense

Manual testing and automated scanning

Automated tools help identify well-known security issues, while manual testing provides a deeper analysis of specific application components and attack surface exploration

Cutting-edge tactics, techniques, and procedures

We apply advanced attacker methods to uncover security gaps, helping to strengthen your application's defenses against real-world threats

Comprehensive security assessment

Our methodology follows industry best practices and standards to detect a wide range of vulnerabilities

OWASP Web Security Testing Guide

OWASP Mobile Security Testing Guide

CWE Top 25
OWASP Top 10

CVSS V3.1

What you get

Objective insights into security threats that could be exploited by attackers to target your application, its users, and your organization

Prioritized list of recommendations to remediate identified weaknesses and enhance the overall security of your application

Detailed breakdown of discovered vulnerabilities, including potential attack scenarios and exploitation paths

43%

High-severity incidents are human-driven attacks according to Kaspersky MDR report; automated tools often miss adversary tradecraft, while security assessments powered by experts reveal critical attack paths for proactive defense

Kaspersky Application Security Assessment

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture