Architecture Risk Analysis

Find and remediate weaknesses in your design before they are exploited.

Identify flaws within a system's design to improve your security posture

Half of the software defects that create security problems are flaws in a system's design. Simply scanning software for security bugs within lines of code or penetration testing applications ignores half the problems that leave an organization vulnerable to attack.

Remediate problems early in your SDLC

By performing security early in the software development life cycle (SDLC), you can avoid the costly rework of addressing security defects found later in the SDLC. Most importantly, finding and remediating security problems earlier in the SDLC is less expensive, less invasive, and less time-consuming than waiting until code is written or QA tests are performed.

Get a clear picture of your risks

In an architecture risk analysis (ARA), Synopsys experts produce a list of technical risks found in your software, and then provide recommendations on the methods, tools, and strategies for mitigating them. We'll also help you understand the related business risks and provide proper mitigation advice to reduce risk to an acceptable level.

Uncover weaknesses in your design

An ARA also reviews your application design in depth to look for weaknesses that might allow attacks to succeed. These design deficiencies are found by analyzing the system's major software components, trust zones, assets, security controls, asset flows, and threat agents. An ARA can discover whether any of your security controls can be bypassed, are weak, or are the wrong controls for what you're trying to achieve.

How an ARA works

An architecture risk analysis consists of four essential steps.

1.