SYNOPSYS®

www.synopsys.com |

Thick Client Testing

Customized to fit the unique needs of your thick client software

Since thick client applications include both local and server-side processing and often use proprietary protocols for communication, they require a different approach to security testing. Simple, automated vulnerability assessment scanning isn't enough. That is why we customize each test to the application.

Our approach is as unique as your thick client software

Our thick client application penetration tests include a risk-based analysis of both the thick client software and server-side APIs that it communicates with. This enables us to identify:

- High-risk areas in the system
- Assets
- Attackers
- Potential attack vectors

Our risk-based approach combines four tracks of analysis

Our thick client software testing process takes a risk-based approach that covers the following four areas:

1. Configuration analysis

Our experts analyze your thick client's configuration, which exposes both default configuration problems as well as ways in which the application could potentially be configured to bypass security controls.

2. Network communication analysis

With many thick clients, most attacks of concern are ones that can be executed remotely. When this is the case, we intercept and analyze network communication in depth.

3. Server analysis

The primary purpose of most thick clients is to expose some server-side functionality. Vulnerabilities in the server-side code are often important because a successful exploit may impact all thick clients or central data stores. We analyze the server software using various manual and automated tools during this phase.

Simple, automated scanning isn't enough.

4. Client analysis

We analyze the thick client software itself using various tools. The activities during this phase are highly dependent on the specific software and attacks of concern, and may include activities such as performing memory dumps, testing IPC channels that may permit privilege escalation, fuzzing file inputs, and in-depth reverse engineering.

Our approach involves creating a penetration test plan that identifies and prioritizes testing scenarios based on risk.

We ride with you until the end

At the end of each assessment we will conduct a read-out call with your development team to walk you through:

- Positive findings
- Prioritized vulnerabilities based on their likelihood and impact if exploited
- Mitigation recommendations for each vulnerability

The Synopsys Difference

Synopsys offers the most comprehensive solution for integrating security and quality into your SDLC and supply chain. Whether you're well-versed in software security or just starting out, we provide the tools you need to ensure the integrity of the applications that power your business. Our holistic approach to software security combines best-in-breed products, industry-leading experts, and a broad portfolio of managed and professional services that work together to improve the accuracy of findings, speed up the delivery of results, and provide solutions for addressing unique application security challenges. We don't stop when the test is over. Our experts also provide remediation guidance, program design services, and training that empower you to build and maintain secure software.

For more information go to www.synopsys.com/software.

Synopsys Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: software-integrity-sales@synopsys.com