



Insider Threat Detection

What hidden threats are lurking under the surface of your code?

We take an innovative, systematic approach to neutralize potential malicious code before it can be activated to trigger an attack or exfiltrate data.

Dive deeper into your code

We combine Static Application Security Testing (SAST) and binary scanning to uncover any code in any part of a software system or script that may appear normal but actually is intended to cause undesired effects such as security breaches or damage to a system.

1. Understand

Our experts conduct client interviews to understand the SDLC and vulnerability management program.

2. Analyze

Our experts analyze the binary or source code through SAST using our own tools to identify points of interest. They also conduct a manual analysis to determine if the points of interest contain potentially malicious code.

3. Recommend

At the end, we compile a final report with points of interest suspected of containing malicious code and a suspicion rating for each. Finally, we provide recommendations to help you choose the best way to resolve them.

We'll help you uncover

- Backdoors
- Cross-organization insider threat actors (aka malicious developers)
- Rootkit-like behavior
- Suspicious constructs in production binaries, configurations, and data
- Time bombs
- Trojan horses

The greatest danger to your software may not be the threats you can see—but the ones you can't.

Our Insider Threat Detection enables you to...

- Find suspicious constructs in production binaries, configurations, and data.
- Identify malicious code that typical security tools won't find because there are no vulnerability markers.
- Discover cross-organization insider threat actors (e.g., system administrator and IT operations, configuration and change management, and developer).
- Get expert advice on appropriate methods of malicious code management and typical vulnerability remediation strategies.

We'll always guide you out of danger

The best part is that we don't just hand over your results and walk away. We explain how and why all suspected points are potentially malicious code, offer advice to help you manage the discovered malicious code, and provide effective vulnerability remediation strategies.

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