Security and the Internet of Things (IoT)

Deliver a sustainable IoT security initiative that provides continuous and comprehensive security risk identification and mitigation

Overview

The Internet of Things (IoT) is transforming entire industries, creating tremendous benefits but also introducing new risks. The security risks surrounding IoT software and applications are snowballing as organizations rush to get devices to the marketplace or into use within the enterprise as soon as possible.

To ensure the safe and reliable operation of billions of IoT-connected devices, organizations must implement IoT security solutions.

With over 20 years as a leader in software security, Synopsys is uniquely positioned to adapt and apply software security best practices to your IoT development initiative, or to help you assess your risk exposure to IoT products within your business.

Why hackers are breaking into IoT devices

Many IoT devices are connected to otherwise secure networks (such as those at large businesses) without the organization fully understanding the scope of the security issue these devices create. This knowledge gap is dangerous because:

- What makes IoT devices smart and able to interoperate with other devices is software.
- If the software on a device is not designed to be secure, it will contain vulnerabilities that attackers can exploit to gain access to the device.
- If attackers infiltrate a device, not only can they access data on that device, but they can also pivot to reach other connected targets on the network, including the back-end application server.

The context has changed, but the rules have not

More and more industries are building IoT devices. But many organizations don't know how to make the software on those devices secure. Fortunately, the fundamentals of software security are the same no matter where the software lives. The experts at Synopsys know how to adapt these security fundamentals to the unique features of the IoT ecosystem to help you get up to speed quickly and achieve a greater maturity level.

4 steps to a successful IoT security solution

Our goal is to help you deliver a sustainable IoT security initiative that provides continuous and comprehensive security risk identification and mitigation. We do this by empowering you to:

- Integrate security into every aspect of your SDLC.
- Educate your developers.
- Implement penetration testing.
- Perform threat modeling.

We have the expertise, tools, and services you need to 'build security in'

Our approach is grounded in the fundamentals of technology risk management, which include:

- **Penetration testing.** Eliminate vulnerabilities in your device, server-side applications, and APIs by testing in QA and production environments.
- **Red teaming.** Ensure your network, physical, and social attack surfaces are secure.
- **Static application security testing.** Quickly scan code and find vulnerabilities using both automated and manual approaches.
- **Architecture and design.** Identify design flaws, which cause 50% of security vulnerabilities.
- **Security training.** Teach your developers the art of coding securely from the start.
- **Program design and development.** Establish and implement governance and processes.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at 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: sig-info@synopsys.com