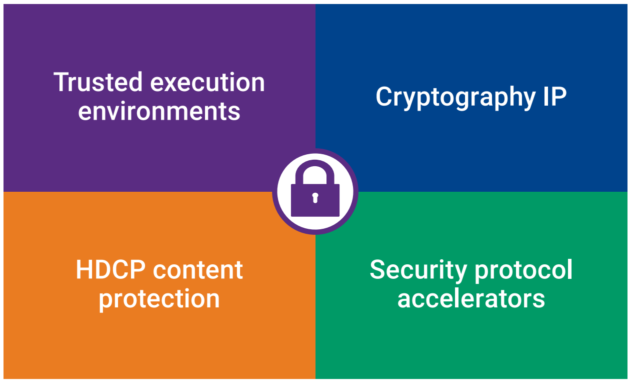
DesignWare Security IP Overview

Enabling the Highest Levels of SoC Security

Secure Your SoC from the Start

Whether you are developing system-on-chips (SoCs) for mobile and wearables, automotive, artificial intelligence (AI), or entertainment, securing your proprietary data and your customers' information is critical to your company's long-term success. Hackers can exploit vulnerabilities in any part of those systems, at the network, device, or chip levels. Protecting your systems starts with having base security functionality hardened into the SoC to enable the setup of a secure communication environment.


Trusted execution environments
Cryptography IP
HDCP content protection
Security protocol accelerators

Broad portfolio of certified and standards-compliant IP solutions

Synopsys' industry recognized security experts are committed to helping you protect your SoC. We provide a broad portfolio of highly integrated security IP solutions that support your system requirements to help you accelerate your secure chip's tape out and time-to-market, even if you don't have in-house security experts. Our IP and software solutions help prevent a wide range of evolving threats in connected devices—threats including theft, tampering, side channels attacks, malware and data breaches.

The reality is, security breaches can affect any connected device. Protect yours with DesignWare Security IP.

Automotive	AI	Industrial	Wearables	Entertainment
• Protect car subsystems and data against tampering • EVITA	• Secure algorithm protection • Avoid rogue data injection	• Remote updates and control • Monitor and manage production flow	• Fast, efficient, seamless ID and authentication • Secure in-field updates	• Ultra HD content protection • Secure key management • Side channel attack resistance

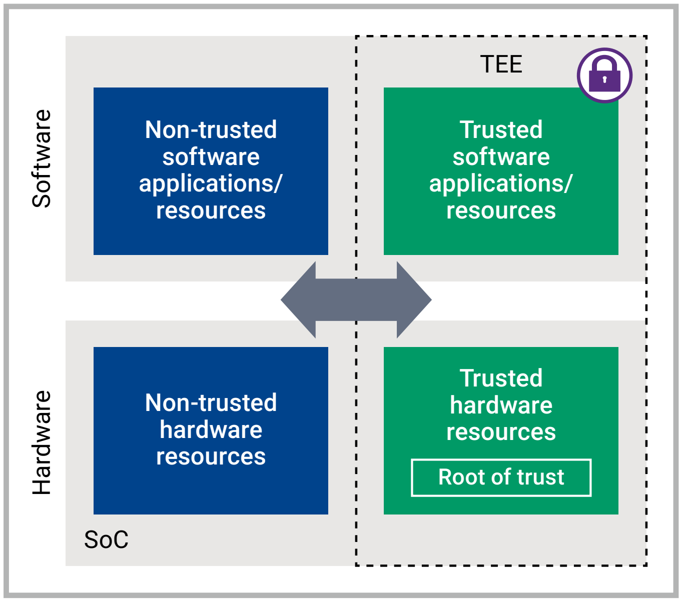
> *"As security attacks increase and evolve, relying solely on internal development carries too much risk and affects time-to-market.*
>
> *We use DesignWare Security IP for our autonomous automotive SoC product lines due to Synopsys' deep security expertise and proven, certified technology that supports the features we require."*
>
> ~VP of ASIC Design, Leading AI Chip Provider

Your SoC Deserves a Unique, Tamper-Proof Identity

Creating trust in devices begins early in the design process and figures in aspects of manufacturing, service and maintenance throughout the devices' life cycle. Many devices store and process valuable information such as service subscriptions, health records, credit card and banking information, and similar data on behalf of their owners that must be protected. Deeply embedded security has never been more critical.

Embedding a hardware root of trust enables chip manufacturers and their OEM/ODM customers to build a trusted execution environment (TEE) to protect valuable data stored within trusted software and hardware resources. The TEE creates a strong cryptographic device identity that is permanently bound to that unique device. Manufacturers can use this trusted identity to provide secure maintenance or enable new features and services. The trust can then be extended to the network and other connected devices.

Synopsys offers several options for creating a TEE on an SoC. The DesignWare® tRoot Hardware Secure Modules (HSMs) with Root of Trust protects sensitive information and data processing within the SoCs. The tRoot HSMs are available either as flexible, configurable HSMs, or as self-contained HSMs for a completely secure environment with a limited set of interactions with the host processor. Designers can also choose ARC® SecureShield™ Technology to build a TEE on low-power ARC EM embedded processors.


TEE
Software
Non-trusted software applications/ resources
Trusted software applications/ resources
Hardware
Non-trusted hardware resources
Trusted hardware resources
Root of trust
SoC

Build a Strong Foundation with Secure Cryptography

The cornerstone of all security solutions that deal with confidentiality, integrity, and authentication is cryptography. Synopsys' DesignWare Cryptography IP, including symmetric and hash cryptographic engines, Public Key Accelerators (PKA) and True Random Number Generators (TRNG), are silicon-proven, standards-compliant solutions providing the essential building blocks of secure systems. The hardware and software security implementations are easily configured, cover a wide spectrum of size and performance combinations, and are available in different architectures, such as look-aside or flow-through. Each cryptographic core can be used as a building block for security protocol accelerators and embedded security modules.

> *"With increased demand for data protection against malicious attacks, we needed to develop our storage SSD SoC with strong security based on proven, standards-compliant IP. Synopsys' DesignWare Security IP enabled us to implement the highest level of security for our SoC."*
>
> ~Sky Shen, CEO of Starblaze

Protect High-Value Digital Content

Designs supporting HDMI and DisplayPort (including USB Type-C connectivity) can ensure the highest content protection between links with DesignWare HDCP Embedded Security Modules. Our proven security solutions span silicon cores to embedded software to help content owners, service providers, network operators, embedded system OEMs and SoC suppliers protect high-value digital content for the home entertainment and digital media markets.

Accelerate Standard Security Protocols

Supporting major security protocols such as IPsec, TLS/DTLS, WiFi, MACsec, and LTE/LTE-Advanced bring complex cost and power requirements to your SoCs. Synopsys' DesignWare Security Protocol Accelerators offer power- and area-efficient encryption and authentication capabilities for your design, providing increased performance, ease-of-use, and advanced security features such as quality-of-service, virtualization, and secure command processing.

> *"Meeting industry security requirements can be challenging, but the Synopsys Security IP was very easy to integrate, allowing us to meet the necessary security standards and performance within the silicon area budget."*
>
> ~Avi Bauer, Vice President of Hardware Engineering at Arbe

Build Safe and Secure Automotive SoCs

The ASIL B Compliant tRoot Hardware Secure Module for Automotive augments its comprehensive root of trust security solution with a suite of automotive documentation and hardware safety mechanisms to protect against both malicious attacks and random and systematic faults.

The tRoot HSM for Automotive safety mechanisms such as dual core lockstep, memory ECC, register EDC, parity, watchdog and self checking comparators, provide protection against permanent, transient and latent faults for the secure system that includes an ARC(R) processor, scalable side-channel resistant cryptography, secure external memory controllers and true random number generator. The ASIL B Compliant tRoot HSM for Automotive is developed and assessed specifically for ASIL B random hardware faults and ASIL D systematic development flow.

Why Choose Synopsys for Security IP?

1. Proven & trusted in 400+ designs
2. Highly integrated
3. Recognized technology leadership

Software Security

In addition to security IP, Synopsys offers the most comprehensive solution for integrating security and quality into your software development life cycle and supply chain. The comprehensive array of managed and professional services, products, and training is tailored to fit your specific needs. For more information on software security, visit synopsys.com/software-integrity.

About DesignWare IP

Synopsys is a leading provider of high-quality, silicon-proven IP solutions for SoC designs. The broad DesignWare IP portfolio includes logic libraries, embedded memories, PVT sensors, embedded test, analog IP, wired and wireless interface IP, security IP, embedded processors, and subsystems. To accelerate prototyping, software development and integration of IP into SoCs, Synopsys' IP Accelerated initiative offers IP prototyping kits, IP software development kits, and IP subsystems. Synopsys' extensive investment in IP quality, comprehensive technical support and robust IP development methodology enable designers to reduce integration risk and accelerate time-to-market.

For more information on DesignWare IP, visit synopsys.com/designware.

SYNOPSYS®
Silicon to Software™

03/29/21.CS665176297_SG | Update Security IP Brochure.