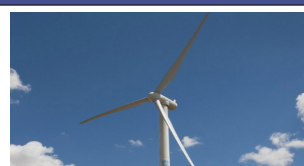# Security Products and Services

Security Challenge

Cyber security threats are becoming more prevalent across commercial industries. The attack vectors constantly evolve, causing a greater need for strong product protection. Failure to protect against cyber security attacks can result in customer dissatisfaction, product recalls, poor Public Relations (PR), and significant financial losses. At the same time, each program has unique security, platform, performance, and business requirements. Security is therefore a strategic and technological problem for product managers and developers. It is generally unfeasible to solve these problems using a single technology. Using an independent systems integrator with mature security products and established expertise is far more effective.

Microsemi® provides security products and services for our industrial clients throughout the program life-cycle. We empower product managers to successfully deploy appropriate countermeasures through the use of skilled security professionals and targeted technologies.

Importance of Security
Failure to protect against cyber security attacks can result in customer dissatisfaction, product recalls, poor PR, and significant financial losses.

The Need for Security
Chinese Corporate Espionage of AMSC Wind Turbine
Unfortunately while the connectedness, distribution, and sophistication of Industrial systems is increasing, security is not.

Products

Microsemi Security Solutions products create layered security over critical program information (CPI) to protect Intellectual Property (IP). Our products enable engineers to efficiently build custom hardware, crypto, and software protection schemes to satisfy security needs.

Hardware Security	EnforcIT® is a set of VHDL IP cores for Microsemi field programmable gate arrays (FPGAs), Xilinx, and Altera. Each IP core can be a standalone protection mechanism mitigating reverse engineering, counterfeiting or tampering attacks. Suite B cryptography cores are FIPS 140-2 certified.
Software Security	CodeSEAL™ secures desktop and real-time embedded operating systems running PowerPC or x86 chipsets against reverse engineering and tampering. Layers of active software security forces adversaries to attack a complex network of countermeasures.
Cryptography	Microsemi's WhiteboxCRYPTO™ product combines mathematical algorithms, data, and code obfuscation techniques to transform the key and related crypto operations in complex ways requiring deep knowledge in multiple disciplines to attack. Importantly, the key is never present in static or runtime memory. Rather, the key becomes an inert collection of data that is useless without the uniquely generated white box algorithm. Support is provided for AES, RSA, ECC, and many other public and custom ciphers. The EnforcIT product includes Suite B, FIPS 140-2 certified cryptography cores.

The Microsemi Advantage	
Skilled Professionals	Microsemi offers a full staff of experienced security professionals including protection engineers, researchers, red-team analysts, software developers, and project managers.
Targeted Security Products	FPGA IP cores, software, and cryptography anti-tamper products along with dedicated security products from partners allow developers to leverage years of experience and efficiently implement comprehensive system protections.

Professional Services

Microsemi's dedicated services are performed by highly skilled services engineers. End-to-end solutions include creating protection plans, developing and implementing protection designs, and executing red-teaming of protected systems to ensure IP is properly protected. We work with product managers and development teams to design protections that leverage characteristics of the underlying platform and to build a robust protection network with no single point of failure.

Risk Assessment Services provide the inputs necessary to identify, scope, and integrate security requirements with program capabilities. A risk assessment supplies information helpful in analyzing costs/benefits, as well as in making critical security decisions to mitigate threats with minimal impact to program cost or schedule. A risk assessment reviews your system in detail to discover vulnerabilities, enumerate threats, and outline the likelihood and consequence of system compromise. These services, performed by engineers experienced in attack tree modeling, reverse engineering, and exploitation tools and techniques, provide the basis for protection planning and security engineering services.

Protection Planning Services help customers step through the life-cycle process to support required inputs for each design review and technical interchange meeting. Our personnel have experience in developing protection plans as well as providing inputs for deliverables. Using a risk assessment and other compiled data, you will receive documentation including a protection design and an implementation approach. The documentation describes how to mitigate identified system vulnerabilities and assesses residual vulnerabilities.

Protection Evaluation Services review the security of your protection design to document vulnerabilities in the exposed system. **Red Teaming Services** start with a black-box approach, pitting experienced reverse engineers with state-of-the-art attack tools against your system in a deployed setting. **Blue Teaming Services** use the same experienced engineers but provide them with full access to documentation, architecture diagrams, and other engineering expertise. A Blue Teaming approach typically reveals flaws in the Protection Design or Protection Implementation. While similar to a Red Teaming exercise, Blue Teams can produce results in a shorter time frame.

Security Engineering Services assists customers by providing an engineering team experienced with the tools, processes, and methods required to analyze, design, implement, and test security features for existing systems to satisfy ever changing protection requirements. Our engineers can develop custom security solutions and novel protection mechanisms that are unique to your application.

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,600 employees globally. Learn more at www.microsemi.com.