Security Solutions

Securing The World's Embedded Systems From Silicon To Software

Hardware, Firmware, and Software

Secure Solid State Drives (SSDs)

Security-Related Services

Cryptography

FPGAs and SoCs

Secure Synchronous Time-Generating Solutions

Microsemi

Power Matters.™

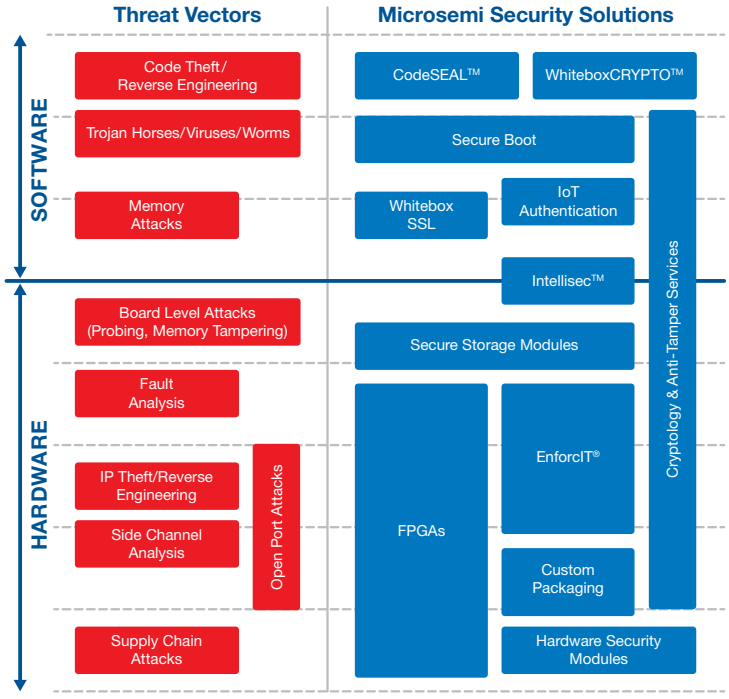
Securing The World's Embedded Systems From Silicon To Software

Hardware, Firmware, and Software Protection For Data-in-Motion, Data-in-Use and Data-at-Rest

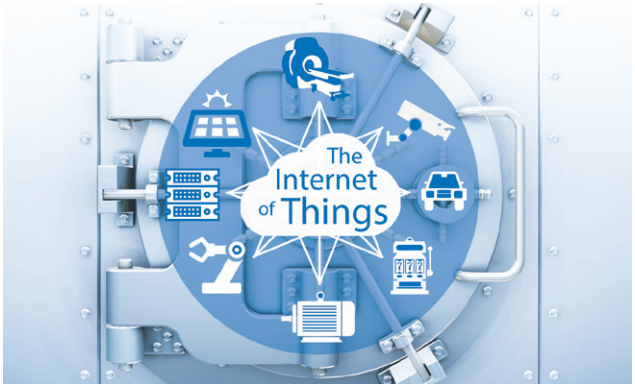
Security needs and cyber threats are growing daily in today's hyperconnected world. Embedded systems, especially as they progressively connect to the Internet of Things (IoT), are deeply ingrained in our daily lives and infrastructure. While this connectivity opens an unprecedented level of efficiency and transparency to many aspects of our lives, having systems subject to increasing digital control also makes them untenably vulnerable to attack.

Cyber threats can emanate from virtually anywhere and include vectors such as:

- IP or theft/reverse engineering
- Trojan horses/viruses/worms
- Memory attacks
- Board level attacks (probing, memory tampering)
- Fault analysis
- Network attacks
- Side-channel analysis
- Supply chain attacks



Consequently, the need to safeguard critical network infrastructure and information systems has never been more imperative. And it is not enough simply to harden the edge of our networks. A layered security approach – encompassing a hardware root-of-trust, security for data-in-motion, data-in-use and data-at-rest, cryptography and software protection – is critical.



Microsemi's security solutions portfolio is specifically aligned to enable this layered approach and weave together the requisite elements to address multiple threat vectors. Our security solutions are broadly used by U.S. federal organizations and commercial entities in applications requiring robust protections such as financial, automotive, medical, digital rights management, gaming, and industrial automation.

Engineered to secure embedded systems from silicon to software, protecting data-in-motion, data-in-use and data-at-rest, Microsemi's security solutions portfolio includes:

Security Solutions:

- Secure Solid State Drives (SSDs)
- Security-related services

Security Applications:

- FPGA/SoC-based Secure Boot
- WhiteboxCRYPTO™
- IoT authentication
- Custom packaging

Security products include:

- Software and Firmware Anti-Tamper IP
- Software, Firmware, and Hardware Cryptography
- FPGAs and SoCs
- Secured Ethernet connectivity ICs
- Secure synchronous time generating solutions

Microsemi is the only commercial company in the Programmable Logic Device (PLD) industry with Defense Microelectronics Activity (DMEA) accreditation for trusted design, brokerage, assembly and test.

To learn more about Micrisemi's security products and solutions for embedded apllictaions, visit: http://www.microsemi.com/applications/security

Unparalleled Data-at-Rest Security with TRRUST-STOR® SSDs

Secure Solid State Drives (SSDs)

Protecting your data-at-rest requires the highest level of information security and performance. Microsemi's high-reliability secure SSDs provide a total data-at-rest solution for embedded computing that can be used in the most demanding settings such as on aircraft, in communications and on missiles. Our secure SSDs, which feature hardware-based encryption and loss prevention, can also be ruggedized and prepared for optimum information assurance.

Microsemi's secure SSD portfolio includes:

- NAND BGA SSDs: Designed for applications where a full-size 2.5" device is too large. Available in two form factors and both PATA and SATA interfaces.
- TRRUST-STOR® SSDs: Originally engineered for defense applications, these high-performance 2.5" SATA SSDs with SLC NAND flash protect sensitive data from environmental and human threats, mitigating vulnerabilities inherent in the memory media.

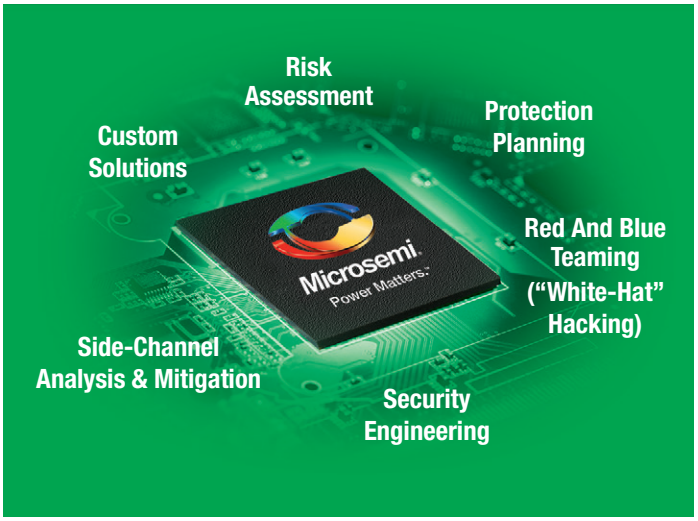
- Secure Encrypting mSATA SLC NAND Flash SSD: A series of micro SSDs forming a complete secure SATA storage system packaged in the industry standard 52-pin MO-300 mSATA form-factor and offering enhanced AES-256 XTS encryption and a multitude of security features unavailable in traditional mSATA SSDs.
- XMC Secure Self Encrypting SSD: An expansion of our secure self-encrypting SSD family in an XMC format.
- SECURRE-Stor™ SATA Encrypted SSDs providing exceptionally secure and reliable data storage for commercial, banking/financial, medical, industrial, smart grid and other critical applications that may currently be using hard disk drives that require physical destruction to prevent data from getting into the wrong hands.

Security Center of Excellence (SCoE)

In response to rapidly evolving cyber threats, Microsemi formed its Security Center of Excellence (SCoE) leveraging more than five decades of extensive embedded systems security experience in the defense market. Our team of security and systems analysts, as well as cryptography, hardware and software engineers, delivers cross-vertical expertise in the security domain for various markets and applications including automotive cyber security, smart grid, defense, financial cloud computing, industrial automation, communications, supply chain assurance and system authentication.

Microsemi's professional security-related service capabilities include:

- Risk assessment
- Protection planning
- Red and blue teaming ("white-hat" hacking)
- Security engineering
- Side-channel analysis and mitigation
- Custom solutions



Microsemi also offers design, assembly, packaging and testing services all in Microsemi's DMEA trusted facility.

Learn more at http://www.microsemi.com/products/solid-state-drives/trrust-stor-ssd

Comprehensive Layered Security Solutions

Anti-Tamper Solutions, Intellectual Property (IP) and Firmware Solutions

According to the U.S. Department of Defense, the best approach for achieving information assurance (IA) in highly networked environments is to utilize a defense-in-depth solution, or castle approach. The defense-in-depth approach places multiple layers of security throughout a system to secure data-at-rest, data-in-use and data-in-motion. Microsemi provides multiple layers of IA and cryptographic technology to secure data-at-rest and data-in-motion in software applications, FPGAs and ASIC designs. Our solutions for end-to-end anti-tamper includes:

- Customizable, NIST certified cryptographic cores enabling encryption, decryption, signing, and verifying of sensitive information.
- A collection of configurable cores ensuring that your critical technologies (CT) are protected from various forms of reverse-engineering and tamper.
- The Shared Memory Protection Suite has been deprecated and should be removed from this presentation.
- CodeSEAL™: Defense-in-depth software application security providing anti-tamper and anti-reverse engineering protections.

EnforcIT provides straightforward integration into existing systems with support for Microsemi SmartFusion and IGLOO FPGAs, Xilinx Virtex and Spartan, and Altera Cyclone and Stratix devices.

Anti-tamper technology is also available in Microsemi's portfolio of SSDs upon request.

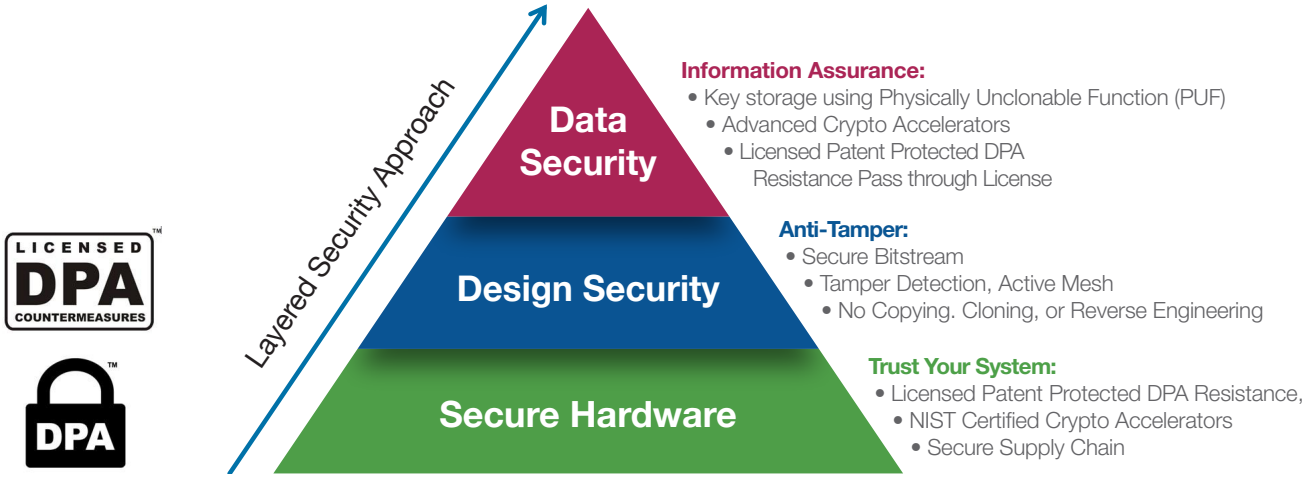
Software, Firmware and Hardware Cryptography

Software cryptography is often a key element in a system's security implementation. While split or key-hiding protection methods can slow attacks, their critical vulnerability lies in the fact that the crypto key can still be compromised when it reassembles in static or runtime memory.

Microsemi can help you secure your data-at-rest and data-in-motion applications with multiple layers of cryptographic technology. Our cryptography solutions include:

- WhiteboxCRYPTO: An innovative, software-based, key-hiding solution forprotection of critical passwords and crypto keys with broad algorithm and platform support.
- WhiteboxSSL™: A drop-in-replacement for OpenSSL using white box cryptography which completely mitigates Heartbleed-like attacks.
- EnforcIT: Designed for flexibility in speed and security, our EnforcIT Cryptography Suite delivers FPGA-based hardware protection and now provides higher assurance with NIST algorithmic certification.

All IP cores are designed for low-risk integration into nearly all standard SRAM or flash-based FPGAs, and can be instantiated into an ASIC design. These and other Microsemi cryptography products are designed and built in the U.S. in Microsemi's trusted facility.



Most Secure FPGA and SoC FPFA Solutions in the Industry

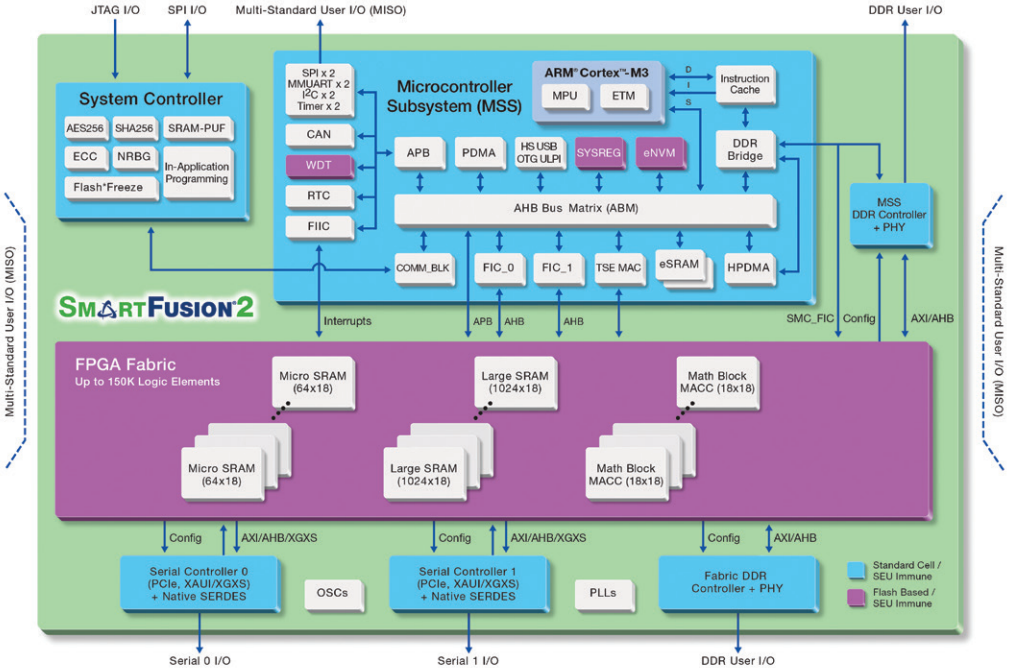
FPGAs & SoCs

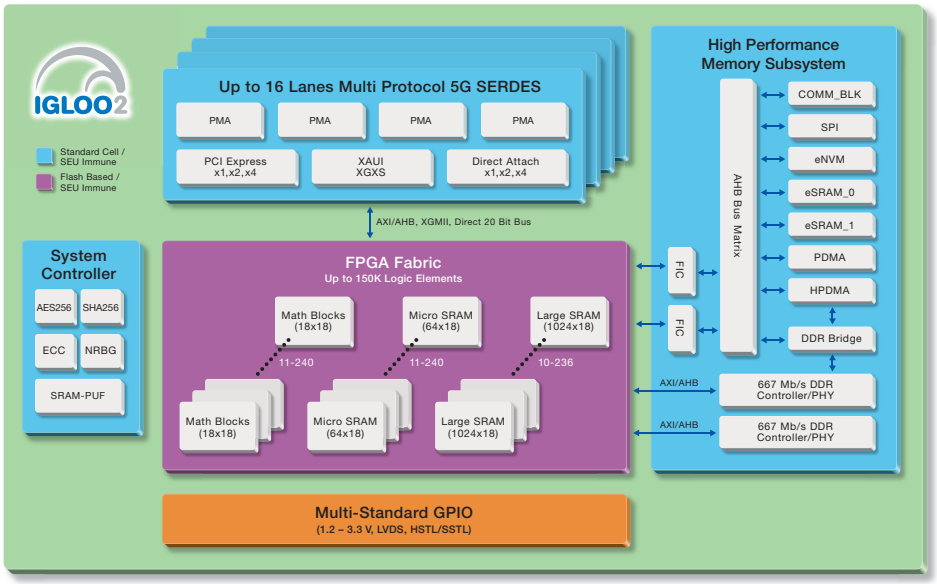
Establishing a system root-of-trust is fundamental to any security scheme to protect critical data from attacks. Microsemi offers the industry's most secure FPGAs with licensed, patented, and certified Differential Power Analysis (DPA) protection to protect your design IP from copying and reverse engineering, built-in certified security functions, as well as supply chain assurance to ensure that the FPGA is authentic. Protecting your data-at-rest or data-in-motion is impossible without secure hardware and design security.

Our flash-based secure boot FPGA and SoC solutions include:

- SmartFusion®2 SoC FPGAs
- IGLOO®2 FPGAs

During programming of Microsemi's IGLOO2 FPGAs and SmartFusion2 SoC FPGAs, the configuration bitstream is authenticated against the parameters certified by the device certificate and the unique device secret key. Using this technique provides the best assurance available that the device being programmed is free from supply chain counterfeiting issues such as upgrading of components, reclaiming and reselling used components as new devices and overbuilding by foundry or test suppliers or rogue insiders. Microsemi's complete IGLOO2 FPGA and SmartFusion2 SoC FPGA anti-counterfeit solution enables true supply chain assurance and system authentication, providing the functions and production controls you need for a complete secure supply chain, from design and fabrication to user programming and deployment to field operation.

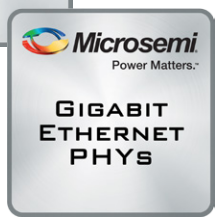




Robust Security Solutions for Network Infrastructure Protection

Secured Ethernet Connectivity

Our increasingly connected world now relies on Ethernet throughout most of the world's wide-area network (WAN) infrastructure to deliver voice, video and data traffic. Standardizing on Ethernet for network communications opens new options for data-in-motion security, since Ethernet networks work at Layer 2 (L2) and have their own encryption protocol defined in the IEEE 802.1AE MACsec standard. L2 security encryption is the ideal choice for secured Ethernet connectivity due to the direct correlation between the strength of the security solution and the layer at which security is implemented.



Microsemi's secured Ethernet connectivity solutions include:

- Gigabit Ethernet (GE) PHYs
- 10GE PHYs

Microsemi's secured Ethernet connectivity portfolio features Intellisec™ IEEE 802.1AE MACsec security, the industry's first technology to enable flow-based IEEE 802.1AE MACsec security encryption end-to-end over any network, including multi-operator and cloud-based networks, independent of the network's awareness of security protocols.

Microsemi's GE and 10GE physical layer devices with Intellisec IEEE 802.1AE MACsec security technology are the world's only PHYs with 128-/256-bit AES encryption technology to have passed FIPS 197 256-bit AES encryption certification. FIPS 197 is a de facto benchmark encryption standard issued by the National Institute of Standards and Technology (NIST) which specifies the approved cryptographic algorithm to protect electronic data. 256-bit AES offers exponentially better data protection with ~10^38 more key possibilities than 128-bit encryption.

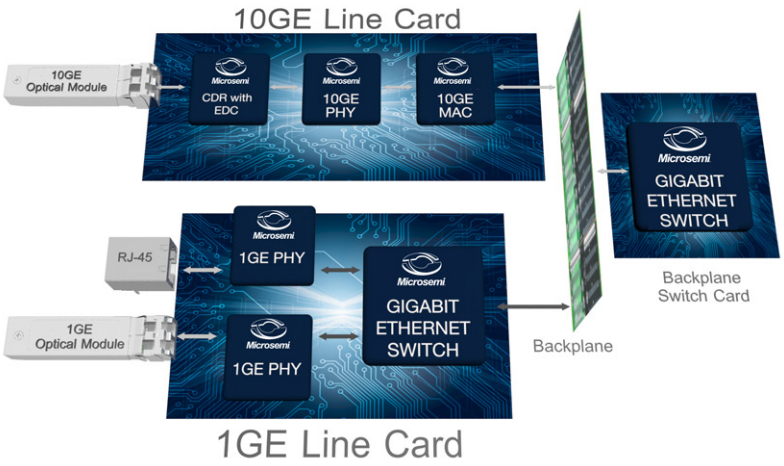
Secure Synchronous Time-Generating Solutions

Timing and synchronization are indispensable in our increasingly digital, networked world. Precise time enables virtually all infrastructures such as data centers, wired and wireless communications, financial exchanges, industrial networks, smart power grid, and other secure communications. Securing synchronous time is vital to protecting critical communications infrastructure, particularly when organizations rely on publicly available time servers acting as sources of Coordinated Universal Time (UTC).

Microsemi is the world leader in network synchronization and precise time solutions, delivering robust network solutions for a comprehensive and secure timing infrastructure. Our end-to-end timing solutions generate, distribute and apply precise time. Microsemi's portfolio includes:

- Timing & Synchronization Systems supporting today's precise timing standards: GPS-based timing, IEEE 1588 (PTP), Network Time Protocol (NTP), Synchronous Ethernet and DOCSIS® timing.
- Clock & Frequency References including hydrogen, cesium and rubidium standards, and quartz oscillators to ensure continuity and integrity of synchronization through GPS outages.
- Timing & Synchronization ICs for clock management (clock synthesis, rate conversion, jitter attenuation and fan-out buffer timing), OTN and packet timing.

For securing Ethernet-based network infrastructure, Microsemi also offers secure IEEE 1588 solutions with its Intellisec PHY, which fully preserve timestamping accuracy on MACsec-enabled links.



Trusted Solutions With Built-In Security

Microsemi has extensive experience with embedded systems security, having served the defense market for over five decades. With cyber security concerns spanning all industries, customers can leverage Microsemi's expertise and capability to build cost-effective, turnkey commercial security solutions. Microsemi provides a broad portfolio of highly integrated component level security and anti-tamper solutions, as well as purpose built modules to meet specific program requirements. Our security solution are widely deployed in multiple sectors, including communications, defense, industrial and the Internet of Things (IoT).

Microsemi is a Defense Microelectronics Activity (DMEA) accredited Category 1A trusted design, test and broker for FPGA and ASIC solutions, complementing our long established trusted assembly and test facility. Our quality and inspection system requirements are certified to MIL-PRF-38534 Class H and K, MIL-PRF-38535 Class Q, ISO 9001:2008 and AS9100.

The only commercial company in the PLD industry with DMEA accreditation for trusted design, brokerage, assembly and test, our areas of expertise include:

- Supply chain assurance
- Anti-tamper response and countermeasures
- Secure packaging
- Threat tree analysis
- Information assurance

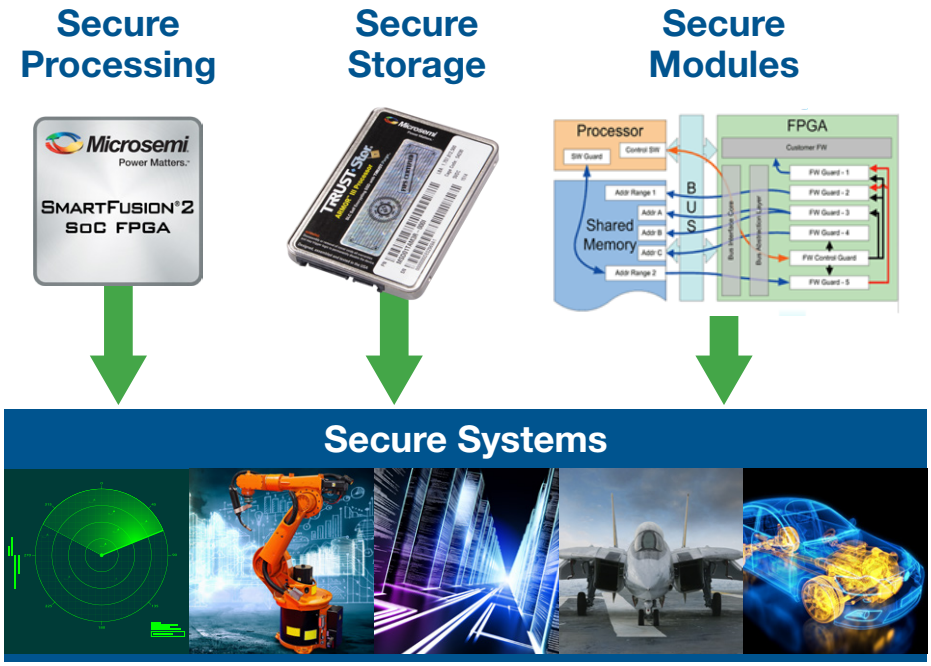
Microsemi has leveraged our expertise and capability from high-grade defense solutions to build cost-effective, turnkey commercial solutions for various markets and applications including automotive, cyber security, smart grid, defense, financial cloud computing, industrial automation, communications, supply chain assurance and system authentication.

Why Choose Microsemi For Your Embedded System Security Needs?

Whatever aspect you're looking to secure, it's important to find a resource you can trust. At Microsemi, we understand the security, performance and reliability imperatives wherever data is collected, communicated or processed, and whenever its accuracy, availability and authenticity are essential. For decades, Microsemi's security experts have provided information assurance (IA) and anti-tamper (AT) solutions and services to safeguard critical program information and technology.

With our industry-leading portfolio including solutions for system trust, securing data-in-motion, data-in-use and data-at-rest, cryptography and software protection, Microsemi simplifies and speeds a customer's path to market with solutions tailored to unique security, platform, performance and business requirements. Robust embedded systems security is within reach.

Contact your local Microsemi sales office today to find the right security technologies, products and services for your design needs.



Microsemi

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo, CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
email: sales.support@microsemi.com
www.microsemi.com

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.

SEC-09-15