COREGUARD®
Protected. Trusted.

FORGET EVERYTHING YOU KNOW ABOUT CYBERSECURITY

CoreGuard® is the only solution for embedded systems that prevents the exploitation of software vulnerabilities and immunizes processors against entire classes of network-based attacks.

DOVER MICROSYSTEMS

COREGUARD®
Protected. Trusted.

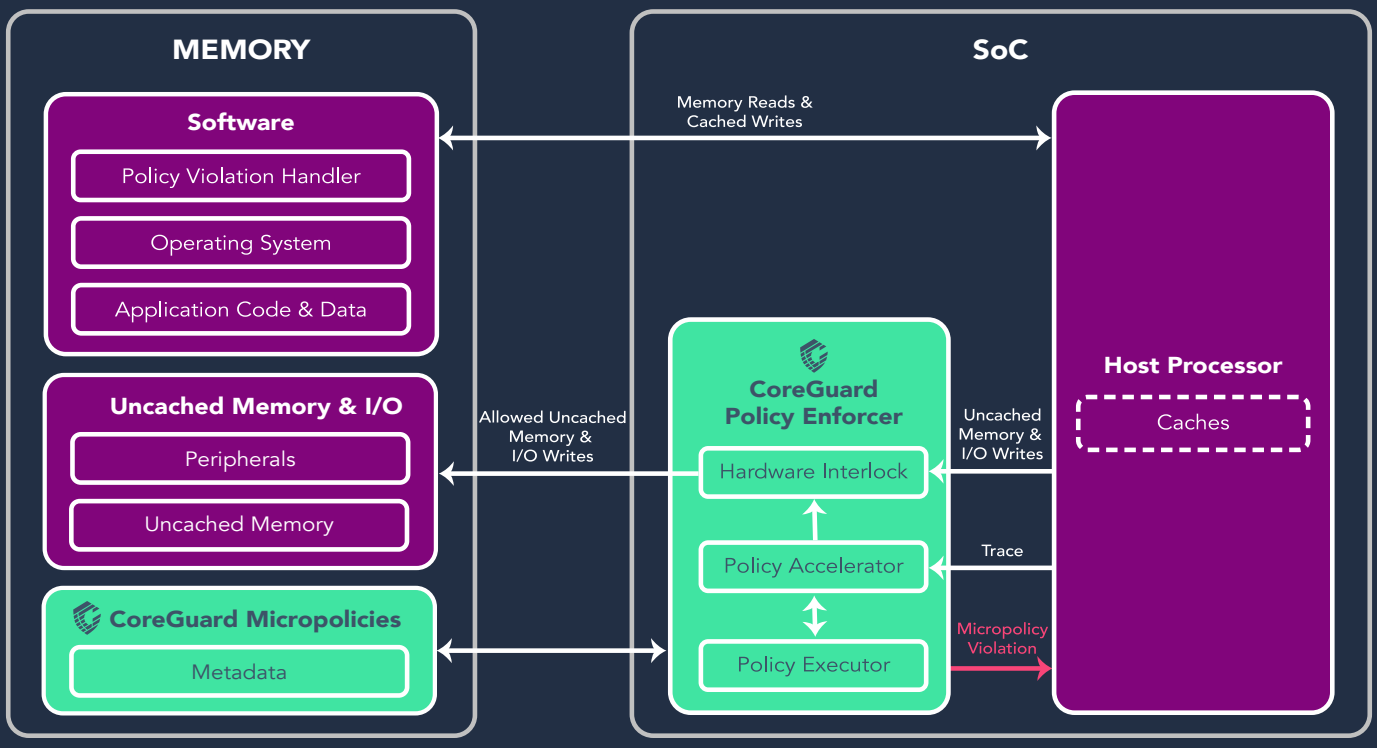
Your processor needs a bodyguard.

CoreGuard silicon IP provides a separate, sentry processor that acts as a bodyguard to the host processor—monitoring every instruction executed to ensure it complies with a set of security, safety, and privacy rules. If an instruction violates an existing rule, CoreGuard stops it from executing before any damage can be done.

HOW IT WORKS

- CoreGuard's **Policy Enforcer** hardware controls communication between the host processor and outside world to ensure nothing sent out peripherals without first being verified.
- Updatable security, safety, and privacy rules, called micropolicies, maintain **metadata** about every piece of data and every instruction processed by the host processor, enabling CoreGuard to distinguish between good and bad instructions.
- **Micropolicies** are designed to stop entire classes of attacks, including buffer overflows, code injection, data exfiltration, and even safety violations.
- The **Policy Executor** administers micropolicies and issues violations. CoreGuard maintains a strict separation between its micropolicy code and metadata, and the application software and operating system. Only CoreGuard hardware can execute CoreGuard micropolicies.

COREGUARD BLOCK DIAGRAM



DELIVERING IOT TRUST

Integrating CoreGuard with embedded processors provides unprecedented IoT security, safety, and privacy.

SECURITY

Prevents against network-based attacks that prey on software vulnerabilities.

SAFETY

Protects against dangerous consequences of device misuse, misconfiguration, and malfunction.

PRIVACY

Ensures private data never gets into the wrong hands.

See CoreGuard in action.

Receive an introduction to CoreGuard and its architecture, take a deep dive into the CoreGuard SDK, and see examples of attacks blocked by CoreGuard.

Request a demo, today!

demo@dovermicrosystems.com

THE COREGUARD ADVANTAGE

IMMUNIZE PROCESSORS

Protects against entire classes of network-based cyberattacks, including zero-day threats.

DEFENSE AGAINST BUGS

The only solution that prevents the exploitation of software vulnerabilities.

SECURITY IN SILICON

CoreGuard cannot be subverted over the network because it is hardwired directly into the silicon

REAL-TIME PROTECTION

Blocks attacks and sends alerts in real-time, before any damage can be done.

CUSTOMIZABLE & UPDATABLE

Micropolicies can be customized to application and securely updated as needed.

SECURITY STACK PROTECTION

Protects the other layers of the cybersecurity stack and eliminates costly signature-based scans.

COREGUARD INTEGRATION

PPA Requirements	
Power	It depends, but CoreGuard adds as few as 153K gates that run at the same speed as your processor with similar toggle rates.
Performance	CoreGuard utilizes a rule cache for negligible system performance impact. With an appropriately-sized rule cache (1K), there is little to no impact on performance.
Area	The area of CoreGuard varies, depending on the type of processor it's protecting, the size of the rule cache, and the size of the metadata tags. The current CoreGuard design can be as low as 153K gates.
Requisite Host Processor Modifications	
Non-Maskable Interrupt (NMI) Input	The processor needs an NMI input; CoreGuard uses this for issuing violations. CoreGuard can use an existing NMI input or a new one can be added.
Instruction Trace Output(s)	The processor needs a set of outputs that provide the Instruction Address (PC), Data Address, and Data Action (load/store) of every retired instruction.
Interrupt Output(s)	The processor needs interrupt outputs that inform CoreGuard of an external interrupt. This enables CoreGuard to context-switch with the host processor to keep interrupt latency low.
System Compatibility	
Processors	Compatible with RISC processors, including Arm and RISC-V. CoreGuard is currently optimized for embedded devices with smaller software stacks.
Operating Systems	Currently supports FreeRTOS version 10. This embedded operating system is shipped with the CoreGuard SDK.
Programming Languages	Supports all applications, including those written in C and C++.
Base Micropolicies (Additional micropolicies available to meet application-specific security, safety, and privacy requirements)	
RWX	Establishes traditional Read/Write/Execute permissions for code and data, but with fine-grained resolution.
Heap	Enforces protection on heap blocks in memory.
Stack	Enforces protection on the stack frame for a function in memory.

DOVER MICROSYSTEMS

ABOUT DOVER MICROSYSTEMS

Dover's lineage began in 2010 as the largest performer on the DARPA CRASH program. In 2015, Dover began development inside Draper before spinning out in 2017.

Based in Boston, Dover is the first company to bring real security, safety, and privacy enforcement to silicon. Dover's patented CoreGuard solution integrates with RISC processors to protect against cyberattacks, flawed software, and safety violations.

www.dovermicrosystems.com