Data Sheet

McAfee Embedded Control for Aerospace and Defense

A single solution for system integrity, change control, and policy compliance

Key Advantages

- Minimize your security risk by controlling what runs on your embedded devices and protecting the memory in those devices.
- Provide access, retain control, reduce support costs.
- Selective enforcement.
- Deploy and forget.
- Make your devices compliance- and audit-ready.
- Real-time visibility.
- Comprehensive audit.
- Searchable change archive.
- Closed-loop reconciliation.

McAfee® Embedded Control for Aerospace and Defense Systems—part of the Intel® Security product offering—maintains the integrity of your system by only allowing authorized code to run and only authorized changes to be made to a system. It automatically creates a dynamic whitelist of the 'authorized code' on the embedded system. Once the whitelist is created and enabled, the system is locked down to the current, known good baseline, and no program or code snippet outside the authorized set can run and no unauthorized changes can be made. We provide the required availability of the mission's operations in distributed control systems environments while providing the security foundations for today's critical avionics, weapons control and electronic warfare, and multilevel secure systems.

McAfee Embedded Control is a small-footprint, low-overhead, application-independent solution that provides deploy-and-forget security on embedded systems by converting a system built on a commercial operating system into a "black box" with the characteristics of a closed proprietary operating system. It prevents any unauthorized program on disk or injected into memory from executing and prevents unauthorized changes to an authorized baseline.

Assured System Integrity

Executional control

With McAfee Embedded Control enabled, only programs contained in the McAfee dynamic whitelist are allowed to execute. Any other programs are considered unauthorized, and their execution is prevented and the failure is logged by default. This enforcement prevents unauthorized programs such as worms, viruses, and spyware from executing illegitimately.

Memory control

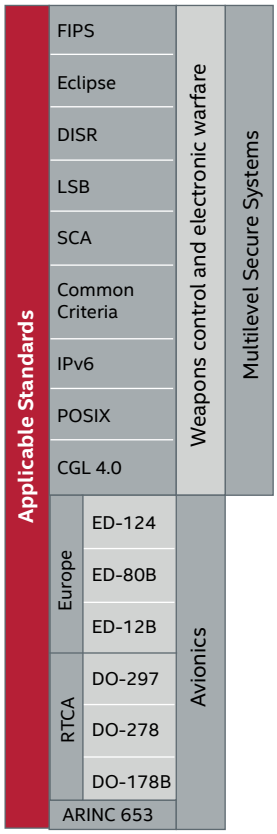
Assures that running processes are protected from malicious attempts to hijack them. Unauthorized code injected into a running process is trapped, halted, and logged. Attempts to gain control of a system through buffer/heap overflow, and similar exploits are rendered ineffective and logged.[1]

Change Control

McAfee Embedded Control detects changes in real time. It provides visibility into the sources of change and verifies that changes are deployed onto the correct target systems. It also provides an audit trail of all changes and allows changes to be made only through authorized means.

intel Security

We Understand the Aerospace and Defense Environment



- FIPS 180-3 compliant.
- Common Criteria-Tested to EAL 3.
- Can be integrated into host-based security systems (HBSS).

McAfee Embedded Control allows you to enforce change control processes by specifying the authorized means of making changes. You may control who (people or processes) can apply changes, which certificates are required to allow changes, and when changes may be applied.

Audit and Policy Compliance

McAfee Integrity Control provides dashboards and reports that help you meet compliance requirements. These reports and dashboards are generated through the McAfee® ePolicy Orchestrator® (McAfee ePO™) console, which provides a web-based user interface for users and administrators. McAfee Embedded Control delivers integrated, closed-loop, real-time compliance and audit complete with a tamperproof system-of-record for the authorized activity and unauthorized attempts.

McAfee GTI Integration: The Smart Way to Deal with Global Threats for Air-Gap Environments

McAfee Global Threat Intelligence (McAfee GTI) is an exclusive McAfee technology that tracks the reputation of files, messages, and senders in real time using millions of sensors worldwide. This feature uses cloud-based knowledge to determine the reputation of all files in your computing environment, classifying them as good, bad, and unknown. With McAfee GTI integration, you'll know with certainty when any malware has been inadvertently whitelisted. The GTI reputation is accessible in Internet-connected as well as isolated McAfee ePO software environments.

Aerospace and Defense—Proven Threats and Needed Protections

Aerospace and defense device developers build large, complex systems on tight and demanding schedules. While you may develop the specifications for your project, it's often impossible to commit resources or build teams until a contract is awarded. Then the clock starts ticking—your team needs to come up to speed quickly. Government standards and certifications have to be addressed. Your piece of the solution must interoperate with all the pieces that other teams are building and tie into the end user's environment. When the technology is mission-critical, your device has to perform with unerring reliability and predictability and cannot allow compromise of data or security on the end-user system. You need to ask yourself these questions:

- How will you deliver new devices on the latest silicon without compromising on safety and security?
- How do you plan to reduce development costs and compress delivery time in the face of increasing systems complexity?
- How will you differentiate your products while meeting strict performance and reliability specifications?
- How will you integrate into your customer's environment and HBSS and FIPs compliance requirements?

Human lives are at stake when it comes to aerospace and defense applications. There is no room for error—safety and security are paramount. Yet time-to-market and increased capability must be achieved. Delivering safe and secure systems in an increasingly complex and connected world is a daunting challenge. Increasingly, the systems in the aerospace and defense arena face significant security challenges from outside threats, especially those that may result in compromising the ability of the system to function when needed and/or loss of data.

During the past decade, the aerospace and defense embedded-software market transitioned to accept commercial-off-the-shelf (COTS) software and now expects the COTS software suppliers to provide solutions for safety-critical environments. This further heightens the security requirements, since the COTS vendors often have not had to grapple with the threat environment of the aerospace and defense arena.

Against this backdrop, the embedded systems world is adopting leading-edge technologies, such as partitioning, virtualization, and multicore to take advantage of more powerful integrated CPUs, multicore and multiple operating system capability, and small and robust separation kernels managing multiple virtual execution environments. There is also increasing demand to run embedded applications on Linux and Microsoft Windows on systems that also have to support safety and/or security functions.

> *"The DoD is responsible for protecting more than seven million machines, linked in 15,000 networks, with 21 satellite gateways and 20,000 commercial circuits. DoD's systems are probed by unauthorized users approximately 250,000 times an hour or over 6 million times per day."*
>
> —Army General Keith Alexander, Head of the US Department, Defense Cyber Command

The continuing demand in the aerospace and defense communities to reduce space, weight, and power (SWaP) as a way of saving costs and increasing payload capability has led to greater reliance on fewer, more powerful embedded computing systems along with greater systems reliability, lower cost of maintenance, and easier upgrade capability for obsolescence management. There is also an accompanying increased demand for security.

With the approval and initial deployment of the Future Combat Systems (FCS) in the US, the NATO Network Enabled Capability (NNEC), and other systems in various countries, the move toward a fully connected military arena is no longer a trend but a reality. This has resulted in:

- Greater connectivity to IP networks for WAN communications.
- Greater connectivity to defense IT infrastructure where threats tend to be more pervasive due to greater IP connectivity and users.
- Greater remote access to the control systems environment.
- Greater sensitivity to use of security technologies that could compromise war fighting ability.

Above all else, nation states must maintain prioritized focus on availability. Ultimately, our enemy's increased interest and their research and knowledge revolves around proprietary control of these embedded systems.

Next Steps

For more information, visit **www.mcafee.com/embeddedsecurity** or contact your local McAfee representative.

About McAfee Embedded Security

McAfee Embedded Security solutions help manufacturers ensure that their products and devices are protected from cyberthreats and attacks. Our solutions span a wide range of technologies, including application whitelisting, antivirus and anti-malware protection, device management, encryption, and risk and compliance—and all leverage the industry-leading McAfee Global Threat Intelligence. Our solutions can be tailored to meet the specific design requirements for a manufacturer's device and its architectures.

Feature	Description	Benefit
	Guaranteed System Integrity	
External threat defense	Ensures that only authorized code can run. Unauthorized code cannot be injected into memory. Authorized code cannot be tampered with.	• Eliminates emergency patching, reduces number and frequency of patching cycles, enables more testing before patching, reduces security risk for difficult-to-patch systems. • Reduces security risk from zero-day, polymorphic attacks via malware such as worms, viruses, and Trojans and code injections like buffer-overflow, heap-overflow, and stack-overflow. • Maintains integrity of authorized files, ensuring the system in production is in a known and verified state. • Reduces cost of operations via both planned patching and unplanned recovery downtime and improves system availability.

(continued)

Feature	Description	Benefit
Internal threat defense	Local administrator lockdown gives the flexibility to disable even administrators from changing what is authorized to run on a protected system, unless presented by an authentic key.	• Protects against internal threat. • Locks down what runs on embedded systems in production and prevents change even by administrators.
Advanced Change Control		
Secure authorized updates by manufacturer	Ensures that only authorized updates can be implemented on in-field embedded systems.	• Ensures that no out-of-band changes can be deployed on systems in the field. Prevents unauthorized system changes before they result in downtime and generate support calls. • Manufacturers can choose to retain control over all changes themselves, or authorize only trusted customer agents to control changes.
Verify that changes occurred within approved window	Ensure that changes were not deployed outside of authorized change windows.	• Prevent unauthorized change during fiscally sensitive time windows or during peak business hours to avoid operational disruption and/or compliance violations.
Authorized updaters	Ensure that only authorized updaters (people or processes) can implement changes on production systems.	• Ensure that no out-of-band changes can be deployed on production systems.
Real-Time, Closed-Loop Audit and Compliance		
Real-time change tracking	Track changes as soon as they happen across the enterprise.	• Ensure that no out-of-band changes can be deployed on production systems.
Comprehensive audit	Capture complete change information for every system change: Who, what, where, when, and how.	• An accurate, complete, and definitive record of all system changes.
Identify sources of change	Link every change to its source: Who made the change, the sequence of events that led to it, the process/program that affected it.	• Validate approved changes, quickly identify unapproved changes, and increase change success rate.
Low Operational Overhead		
Deploy and forget	Software installs in minutes, no initial configuration or setup necessary. No ongoing configuration necessary.	• Works out of the box. Effective immediately after installation. Does not have any ongoing maintenance overhead, thereby a favorable choice for a low operating expense (OPEX) security solution configuration.
Rules-free, signature-free, no learning period, application independent	Does not depend on rules or signature databases, and is effective across all applications immediately with no learning period.	• Needs very low attention from an administrator during server lifecycle. • Protects server until patched or unpatched server with low ongoing OPEX. • Its effectiveness does not depend on quality of any rules or policies.
Small footprint, low runtime overhead	Takes up less than 20 MB disk space. Does not interfere with application's runtime performance.	• Ready to be deployed on any mission-critical production system without impacting its run-time performance or storage requirements.
Guaranteed no false positives or false negatives	Only unauthorized activity is logged.	• Accuracy of results reduces OPEX as compared to other host intrusion prevention solutions by dramatically reducing the time needed to analyze logs daily/weekly. • Improves administrator efficiency, reduces OPEX.

1. Only available on Microsoft Windows platforms.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

60743ds_embedded-control-aerospace_1213B