McAfee Embedded Control for Consumer and Home Networking

Secure digital home devices

McAfee® Embedded Control for consumer and home networking—part of the Intel® Security product offering—maintains the integrity of your system by allowing only authorized code to run and authorized changes to be made to a system. It automatically creates a dynamic whitelist of authorized code on the embedded system. After the whitelist is created and enabled, no program or code snippet outside of the authorized set can run and no unauthorized changes can be made. Intel Security provides complete security to protect individuals using networking devices in their digital homes.

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 unauthorized programs from executing and any unauthorized changes to the system.

Memory control
McAfee Embedded Control ensures 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 overflows and similar exploits are rendered ineffective and logged.

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

McAfee Embedded Control allows you to enforce change control processes by specifying which people or processes can apply changes, which certificates are required to allow changes, what types of changes are permitted, and when changes can be applied.

Assured System Integrity

Executional control
With McAfee Embedded Control enabled, only programs contained in the dynamic whitelist are allowed to execute. All other programs are considered unauthorized, their execution is prevented, and the failure is logged. This prevents unauthorized programs that install themselves—such as worms, viruses, and spyware—from executing illegitimately.

Memory control
McAfee Embedded Control ensures 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 overflows and similar exploits are rendered ineffective and logged.

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

McAfee Embedded Control allows you to enforce change control processes by specifying which people or processes can apply changes, which certificates are required to allow changes, what types of changes are permitted, and when changes can be applied.

Organizations Shaping the Digital Home

Home Gateway Initiative
Home gateway specifications to ensure interoperability.

Broadband Forum
More than 100 specifications of IP networks, including the remote management protocol of the digital home.

Digital Living Network Alliance
More than 245 companies comprise DLNA and drive and support the DLNA standards.

OSGi Alliance
Worldwide consortia that provides specifications, reference implementations, test suites, and certification to create a market for universal middleware.
Audit and Policy Compliance

McAfee Integrity Control provides dashboards and reports to help you meet compliance requirements. These reports and dashboards are generated through the McAfee® ePolicy Orchestrator® (McAfee ePO®) console, which provides a web-based interface for users and administrators.

McAfee Embedded Control delivers integrated, closed-loop, real-time compliance and auditing capabilities within a tamperproof system that records all activity and prevents unauthorized changes.

Consumer and Home Networking—The Digital Home

Internet capabilities have become pervasively embedded in many household devices. As a result, we now expect a seamless, high-quality experience at every interaction point and complete security in all aspects of this experience.

Consumer and home networking devices are proliferating at a tremendous rate. For example:

<table>
<thead>
<tr>
<th>Broadband Access CPE</th>
<th>Residential gateways, xDSL modems and routers, broadband routers, VoIP routers and phones, optical network units (ONUs) and passive optical networks (PONs), femtocells (LTE and WiMAX), and home network-attached storage (NAS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Audio and Digital Video</td>
<td>Set-top boxes (STBs), including satellite, terrestrial, and cable; IPTV and IP STBs (STBs with IP connectivity), digital TV, Internet TV, DVD players and recorders, Blu-ray players and recorders, hard disk recorders, and digital video recorders</td>
</tr>
<tr>
<td>Other</td>
<td>Emerging consumer devices, photo frames, door phones, and home security networks</td>
</tr>
</tbody>
</table>

The proliferation of consumer and home networking devices is driven by several trends shaping the industry.

First, wired and wireless broadband are growing rapidly on a global basis:

- There are more than 500 million broadband subscribers worldwide; they are increasingly using IP-based next-generation networks (NGNs).
- Wireless broadband is taking off in many countries where 3G/3.9G/4G or Wi-Fi/WiMAX networks are used as an alternative or supplement to fixed-line broadband access.
- Forward-thinking countries are also implementing policies to accelerate wired and wireless broadband and develop digital communications and broadcasting.

Not surprisingly, as aggregate device connectivity to the Internet and home networks grows, we’re seeing rapid convergence across the device spectrum. For example, routers are being integrated with modems, access points, and media gateways; set-top boxes are being integrated with media players; and vendors are offering a growing number of devices that deliver voice, data, and multimedia services.

Interoperability is becoming critical as home devices increasingly need to connect with each other. The Digital Living Network Alliance (DLNA) interoperability protocol, the global de facto standard, is supporting and driving this interoperability.

Content and services for the digital home are increasingly diversified, sophisticated, and open. Websites like YouTube, Hulu, acTVila, Philips Net TV, and BBC iPlayer attract millions of viewers, and technologies that deliver Internet content and web applications to home devices are rapidly maturing.

Changing social norms such as social networking, e-commerce, virtual worlds, remote healthcare, online gaming, and media streaming are leading to increased demand for enhanced applications and services that deliver a high-quality, well-designed user experience.

And now the onslaught of cloud computing is accelerating all aspects of home networking and the digital home.

Despite its many benefits, the new digital home also poses tremendous security threats since critical financial, health, and personal data are conveniently accessible to hackers who will unrelentingly seek to burglarize digital content.
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 white-listing, 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.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Guaranteed System Integrity</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 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, Trojans; 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. |
| 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. |

(continued)
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time change tracking</td>
<td>Track changes as soon as they happen across the enterprise.</td>
<td>• Ensure that no out-of-band changes can be deployed on production systems.</td>
</tr>
<tr>
<td>Comprehensive audit</td>
<td>Capture complete change information for every system change: who, what, where, when, and how.</td>
<td>• An accurate, complete, and definitive record of all system changes.</td>
</tr>
<tr>
<td>Identify sources of change</td>
<td>Link every change to its source: who made the change, the sequence of events that led to it, the process/program that affected it.</td>
<td>• Validate approved changes; quickly identify unapproved changes; increase change success rate.</td>
</tr>
<tr>
<td>Deploy and forget</td>
<td>Software installs in minutes, no initial configuration or setup necessary. No ongoing configuration necessary.</td>
<td>• Works out of the box. Effective immediately after installation. Does not have any ongoing maintenance overhead—a favorable choice for a low OPEX security solution configuration.</td>
</tr>
<tr>
<td>Rules-free, signature-free, no learning period, application independent</td>
<td>Does not depend on rules or signature databases; is effective across all applications immediately with no learning period.</td>
<td>• 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.</td>
</tr>
<tr>
<td>Small footprint, low runtime overhead</td>
<td>Takes up less than 20 MB disk space. Does not interfere with application's runtime performance.</td>
<td>• Ready to be deployed on any mission-critical production system without impacting its run-time performance or storage requirements.</td>
</tr>
<tr>
<td>Guaranteed no false positives or false negatives</td>
<td>Only unauthorized activity is logged.</td>
<td>• 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.</td>
</tr>
</tbody>
</table>

1. Only available on Microsoft Windows platforms.