Choosing Between Whitelisting and Blacklisting – Endpoint Security Software for Fixed Function Devices

McAfee* application whitelisting combined with Intel® vPro™ technology can improve security, increase manageability and lower support costs.

SOLUTION BRIEF
Intel® vPro™ Technology
McAfee® Endpoint Security Software
Fixed Function Devices

Introduction
Despite continuing debate over whether blacklisting or whitelisting software is better for securing endpoints, the merits of the two approaches are relatively clear for fixed function devices. This is because devices, such as point-of-sale (POS), medical equipment, industrial control systems and aeronautical systems, generally run a pre-defined set of applications. This attribute favors whitelisting when the main objective is protecting the device, as in neutralizing malware. When it’s necessary to protect a device against infected data – at rest or in transit – blacklisting is needed to find the viruses and counteract them. Here are some simple definitions to level set this discussion:

Blacklisting, also referred to as anti-virus (AV), is a traditional security approach that blocks, and often eradicates, malicious code or data containing a known or suspicious character string documented in a regularly updated malware signature file (i.e., blacklist).

Whitelisting maintains a carefully controlled list of permitted, trusted code (i.e., whitelist), which is allowed to execute, while unknown or unauthorized software is prevented from running.

With cyber attacks escalating and dangerous Stuxnet-class threats on the rise, the security posture of fixed function devices is a growing concern for IT managers. Whitelisting, though not as widely used as blacklisting, provides some significant security and cost advantages. This solution brief compares these two endpoint security software options and suggests how IT managers can stipulate security requirements in requests for proposal (RFP) for fixed function devices or seek out devices with robust security solutions. Supporting both whitelisting and blacklisting models, McAfee* Embedded Control, along with Intel vPro™ technology, enables industry-leading security protection and remote management.
Increasing Risk

There was a time when few worried about the security on fixed function devices, like equipment on an assembly line, kiosks or multi-function printers. But now there is greater risk as modern devices are becoming more connected and are communicating across all types of networks – device, SCADA and even corporate – thus increasing exposure to malware. Therefore, it’s prudent to secure any fixed function device before allowing it to access the corporate network.

Zero-day Attacks

Stuxnet, a sophisticated cyber weapon that targeted and sabotaged automated uranium enrichment facilities in Iran, changed the scope and context of control system cyber security forever. Stuxnet raised the bar by combining stolen certificates and multiple zero-day exploits to deliver a payload that was designed to find and disrupt a specific industrial control process. That payload was also unique, in that it targeted programmable logic controllers (PLCs) used within the automation system – assets that were thought to be untouchable due to their isolation, obscurity and specialized functions.

Zero-day attacks can be averted with specialized application whitelisting security software and memory protection, both of which are particularly effective because they do not need prior knowledge about a piece of malware in order to prevent it from executing or performing buffer overflow tactics. When a new threat emerges and attempts to run, the whitelisting software will discover it is not on the list of trusted applications and block it; subsequently, the incident is recorded in the event log, thereby alerting the endpoint management software, as depicted in Figure 1.

In contrast, blacklisting software can only protect against such an attack after it’s been discovered and a corresponding virus detection signature has been distributed. Moreover, blacklisting solutions are difficult to keep current in these environments; and as a result, devices may rely on outdated signature files that impair the ability of anti-virus solutions to detect and remediate malware. There is a similar concern for devices running legacy operating systems that are no longer supported with regular security patches.

While Stuxnet targeted a particular supervisory control and data acquisition (SCADA) system, it proved to be a threat class that puts many networked systems at risk. To address this risk, McAfee is working with leading control system vendors—including Siemens*, Schweitzer Electric Corporation, Invensys*, Emerson*, Rockwell Automation*, ABB*, Yokogawa* and others—to validate key security technologies and develop a cohesive control system cyber security solution. A major element of this solution is application whitelisting.

Different Security Objectives

When deciding whether to employ whitelisting, blacklisting or both on a fixed function device, it is useful to consider two common objectives:

Device protection: Prevent malware from compromising the device and impairing its operation or using it as a launch pad for other attacks.
  - Advantage >> Whitelisting
    - Capable of protecting against zero-day threats
    - Relatively lightweight

Data protection: Safeguard the data the device touches (at rest or in transit)
  - Advantage >> Blacklisting
    - Anti-virus software performs remediation after a virus is detected

![Figure 1: Application Whitelisting Flow](image)
Comparing Whitelisting and Blacklisting

When selecting a security solution, there are many attributes to evaluate, some of which will be deployment-specific. In a generalized way, Table 1 compares whitelisting and blacklisting for several important considerations associated with fixed function devices. Overall, whitelisting can offer advantages with respect to network and device performance, and IT support effort.

**Whitelisting Support Model**

In general, application whitelisting on fixed function devices requires minimal support effort. A manufacturer may ship devices with whitelisting pre-installed and ready to run so an IT department doesn’t have to do anything but respond to alerts sent by the device. Some devices, such as kiosks in a retail environment, may require infrequent software updates; in that case, an IT department may use a third party agent, like Microsoft* System Center Configuration Manager (SCCM) or IBM* Tivoli* Endpoint Manager, to manage the list of trusted applications permitted to run on the device, as illustrated in Figure 2.

In this example, an authorized administrator defines trusted update sources—including authorized users, application publishers and file servers—and sets up mix-and-match relationships among them. By authorizing a trusted file server, a controlled system could download application patches from a centralized system without an extra approval step. Alternatively, a trusted user could download, install or run a trusted class of application from a trusted publisher, such as a third party agent. A straightforward process can be created that keeps the administrator from becoming a bottleneck and requires little or no ongoing maintenance after the initial setup.

### Table 1: Whitelisting and Blacklisting Comparison

<table>
<thead>
<tr>
<th>IT Considerations</th>
<th>Comparison</th>
</tr>
</thead>
</table>
| **Impact on network performance** | Advantage >> Whitelisting  
Frequent virus signature file updates may consume considerable network bandwidth. |
| **Device performance degradation** | Advantage >> Whitelisting  
A device may lack the CPU performance, memory and storage to handle a comprehensive blacklisting solution. |
| **Out-of-date patches** | Advantage >> Whitelisting  
A device may become vulnerable due to infrequently applied operating system and application patches. (e.g., end-of-life OS, inaccessible device) |
| **Zero-day attacks** | Advantage >> Whitelisting  
This class of attack is difficult to counteract. |
| **IT support** | Advantage >> Whitelisting  
Many IT support hours may be needed to send virus updates, sometimes carried out on a daily basis. |
| **Device Cleansing** | Advantage >> Blacklisting  
When a virus is detected in a file, it is desirable to clean the data. (i.e., continually scan for viruses and eradicate them) |

*In that case, an IT department may use a third party agent, like Microsoft* System Center Configuration Manager (SCCM) or IBM* Tivoli* Endpoint Manager, to manage the list of trusted applications permitted to run on the device, as illustrated in Figure 2.*

**Figure 2: Enterprise Console Updates Trusted Applications**

1. Authorized User Update  
2. Authorized Administrators  
3. Authorized Third-Party Agents, e.g., Tivoli*, SMS*  

Secure Signal Updates
Security Solutions for Fixed Function Devices

McAfee offers a suite of products for securing endpoint devices that can be tied together and integrated with other security and IT systems through the open platform of McAfee ePO (McAfee ePO*). The software enables IT organizations to centrally manage security and achieve dramatic efficiencies. Used on nearly 60 million nodes, the software increases overall visibility across security management activities, thereby improving protection. In addition to being one of the most advanced security management solutions available, McAfee ePO has special capabilities that better secure energy assets:

McAfee* Embedded Control

McAfee Embedded Control automatically creates a dynamic whitelist of the “authorized code” on the device. Once the whitelist is created and enabled, the system is locked down to the known good baseline. No program or code outside the authorized set can run, and no unauthorized changes can be made. When untrusted software attempts to execute, an alert is sent to McAfee ePO, prompting potential corrective action.

While preventing execution of unauthorized code—untested patches, scripts, malware, unapproved applications—McAfee Embedded Control also ensures that authorized code cannot be tampered with by preventing changes to selected files, directories and registry keys. For this reason, vulnerabilities in authorized code cannot be exploited, so the device is safe even when it is unpatched. This benefit is crucial to the security of fixed function devices running legacy operating systems.

Memory protection insulates running processes from malicious hijacking; unauthorized code injected into a running process is trapped, halted and logged. This way, attempts to gain control of a system through buffer overflow, heap overflow, stack execution, and similar exploits are rendered ineffectual and are logged. Authorized updating mechanisms allow granular and selective change control by trusted updaters.

For example, the system might approve Microsoft Windows* patches automatically, while preventing changes to critical device configuration files and logging any attempts. Authorized updating can occur by opening an update window and authorizing a user or application to make changes.

In addition, the system tracks any authorized changes in real time, allowing automatic and accurate monitoring and reporting of actual changes. This provides visibility into the sources of change and verification that changes were deployed onto the correct target systems. Protection is linked directly to policy, and changes are verified against the change source, time window or approved change ticket.

Changes that are attempted outside of policy are not allowed, and attempts are logged. In the event of forensic investigation, activity monitoring can easily identify the time and source of changes, files that were changed, and the user logged into the system at that time.

McAfee* ePO* Deep Command

Lowering the cost to service endpoints, this solution minimizes expensive onsite visits to address security incidents or equipment failure. Security administrators can deploy, manage and update security and device software on disabled or powered-off endpoints. McAfee ePO Deep Command employs Intel vPro technology, which establishes an out-of-band (OOB) connection to the endpoint that allows IT departments to take control of the device – even a rogue device - regardless of the hardware or software state. Using Intel vPro technology, the device can be taken offline, cleansed remotely by reloading its software image and then brought back online.
Hardware-Assisted Security

In addition to the protection provided by current software solutions, Intel vPro technology-enabled solutions provide hardware-based mechanisms that help protect against software-based attacks, and protect the confidentiality and integrity of data. They do this by enabling an environment where applications can run within their own space, protected from all other software on the system. These capabilities, enhanced by hardware-assisted Intel® Virtualization Technology (Intel® VT), provide the protection to mechanisms, rooted in hardware, that are necessary to provide trust in the application’s execution environment. In turn, this can help to protect vital data and processes from being compromised by malicious software running on the platform.

Embedded devices with Intel vPro technology also include industry standard Trusted Platform Module (TPM) 1.2, which stores keys in hardware, so security measures such as hard-drive encryption (for example, via McAfee Total Protection for Data) are more effective.

Platforms based on Intel vPro technology also support hardware-assisted encryption and decryption that is accessed via Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI). In benchmark testing, files can be decrypted almost thirteen times faster than previous software implementations. For more information, click here.

Insist on Better Device Security

With dangerous cyber threats escalating, IT managers can ill-afford leaving device security to an afterthought. It’s critical to have early discussions with device manufacturers to specify requirements in a request for proposal (RFP) or product purchasing agreement. If purchasing off-the-shelf products, seek out ones that have a comprehensive security solution. When a fixed function device is based on an Intel® processor, stipulate a robust whitelisting solution, including:

- McAfee Embedded Control with application whitelisting
- McAfee ePO Deep Command
- A computing system based on Intel vPro technology

---

1 Intel® Virtualization Technology (Intel® VT) requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM), and for some uses, certain platform software enabled for it. Functionality, performance, or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

2 Performance results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance.

Copyright © 2012 Intel Corporation. All rights reserved. Intel, the Intel logo, and Intel vPro are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others. Printed in USA 0612/TB/TM/PDF Please Recycle 327608-001US