Process Solutions

White Paper

Staying Ahead of Today’s Cyber Threats

Executive Summary

In an age where ubiquitous flash drives can become precision-guided munitions and a serious security breach is a single, misguided decision away, the concept of “defense-in-depth”—employing multiple layers of both physical and cyber security measures—has become a prerequisite for maintaining operations.

Table of Contents

The increasing complexity and volume of applications, and the issues stemming from threats to these applications, requires continuously evolving approaches and tools to combat potential attacks. For example, McAfee reported unprecedented growth in detected malware[1] and suggested the total number of pieces of malware in their database will grow at a rapid pace.

Such statistics further emphasize that the security-threat landscape continues to evolve. So too must the tools that combat those threats.

To that end, one development in cyber security protection is the concept of application whitelisting—an approach used to combat viruses and malware, allowing "safe" software to operate while blocking other, potentially unsafe applications. The basic concept behind application whitelisting is to permit only good known files to execute, rather than attempting to block malicious code and activity. When properly implemented, it should:

- Enforce a list of approved applications,
- Include an administration tool that allows for adjustment to the whitelist, and
- Monitor, block and report attempts to run unapproved files

With increasing numbers of attempted intrusions, cautionary tales of security breaches and the potential for resulting damages at various sites, application whitelisting can be an important addition to a utility's security arsenal. But before being implemented it is important to understand the security landscape and how whitelisting can fit into a utility's security strategy.

Application Whitelisting 101

Application whitelisting accomplishes its objectives by creating a list of approved software and applications and allowing only those to execute. Email management, for instance, is a common application of a whitelisting technique. Spam is eliminated from inboxes while safe correspondences are allowed access. This approach is in contrast to blacklisting—one approach used by anti-virus software, which is a standard, signature-based approach that blocks or removes known harmful software.

Blacklisting, while effective, has a weakness in that it only blocks known bad actors—leaving a time gap between the detection of a new piece of malware and the inclusion of its signature in the latest update from the anti-virus vendor. During that time gap, there is a window of exploitation where a system may be vulnerable to the new malicious code. Malware examples, such as worms and trojans, utilize signature-morphing methods that can bypass traditional anti-virus detection. Application whitelisting does not depend on known malware signatures, so it provides greater protection against new malware without requiring signature updates.

While the general concept of whitelisting is simple, integrating it into an Industrial Control System (ICS) can be risky. Whitelisting must be tightly integrated into an ICS, and thoroughly validated so that it does not impact performance, or block critical system functionality under any circumstances. Most whitelisting solutions include a monitor-only mode, which enables a managed, low risk approach to incorporating whitelisting protection on an ICS.

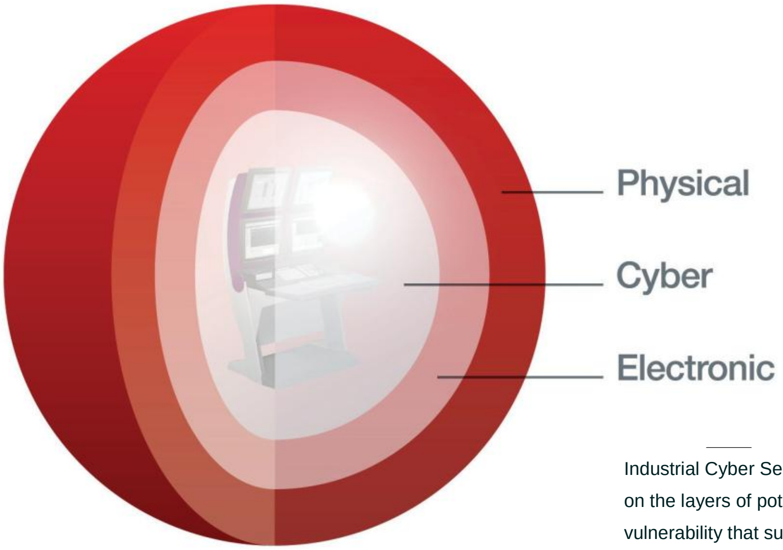
Application whitelisting technology continues to improve, with most vendor solutions offering a variety of additional protective features beyond file execution protection. These features include device protection for USB and CD/DVD devices, registry protection, file verification against an off-site master file database, protection of non-executable files, increased protection against memory-based malware, and baseline tracking of all files on a system. Some whitelisting solutions integrate with other security tools to provide a larger view of the security landscape of the system. Whitelisting can significantly simplify certifying system compliance and change management. With careful planning, whitelisting solutions can provide benefits far beyond just restricting file execution to known good or approved files.

Including the IT Perspective

Whitelisting was designed and architected for the enterprise, or business IT environment. Priorities for operating in a business IT environment are different than those for an industrial control system. Confidentiality, Integrity, and Availability of data are primary concerns in defining the security of a system. Maintaining data confidentiality and integrity are the highest priority requirements for a business IT environment. On an industrial control system, data availability is the highest priority. Industrial control systems provide some unique challenges for whitelisting products and other security solutions, including:

- High availability requirements of the system—limited update opportunities
- High risk of changes impacting process operation—slow to implement patches and updates
- Industry and government standards compliance requirements
- Legacy systems running older operating systems

Therefore, business IT security solutions which are deployed on industrial control systems have to be adjusted to accommodate the operational requirements of an ICS.



Industrial Cyber Security focuses on the layers of potential vulnerability that surround the control system.

Figure 1: Layers of vulnerability in control systems

There are several approaches in getting the IT and control systems departments on the same page. Mingling departments, for instance, is an effective method of ensuring successful communications. Assigning IT workers to the process engineering department and vice versa can help the two organizations come to a better understanding.

Activities designed to bring the two groups closer is also effective. Seconding an IT worker to the controls group allows them to gain a different perspective and appreciate the priorities of engineering and, when the seconded employee rotates back to the original IT group, they will bring with a shared experience with added perspective. Situating the two groups in the same room and including both groups in meetings can also promote cross-group harmony.

By sharing information, collaborating and communicating between both IT specialists and process engineers, companies can achieve solutions that incorporate a bevy of viewpoints and better protect themselves against costly safety and security incidents that impact their bottom lines.

Where Does Whitelisting Fit in the Lifecycle?

It is also important to understand where whitelisting fits within the industrial cyber security lifecycle. Taking a logical approach to managing this lifecycle is key to securing the critical infrastructure.

This is a process with four distinct phases—assessment, remediation, management, and assurance. Each phase in the lifecycle is important, but the assessment phase is perhaps the most revealing. Assessing assets and vulnerabilities against industry standards and best practices provides a roadmap to eliminating or diminishing revealed areas of risk.

During the assessment phase, the applicability, deployment strategy and proper selection of technologies like application whitelisting will be defined. In future assessments the effectiveness of the protection technologies will be evaluated to ensure they continue to meet the site's security needs.

The remediation phase begins by addressing vulnerabilities and alignment with industry standards and best practices. A custom-designed security program is one of the deliverables from this phase. This is the phase of the security lifecycle in which application whitelisting and other protective technologies will be deployed.

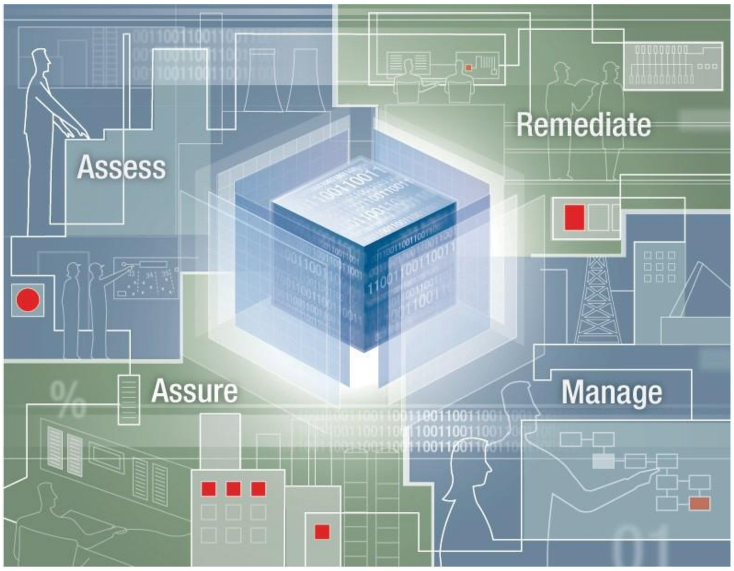


Figure 2: Four distinct phases of securing critical infrastructure

Once remediation has occurred, it is necessary to keep the network and security programs at their optimum level. This activity occurs in the management phase of the industrial cyber security lifecycle. In this phase, the focus is on preserving and enhancing the investment made in security, by applying services and training. Ongoing management of systems and technology would include anti-virus and patch management services and network perimeter management.

The assurance phase requires the integration of multiple data sources along with the tools and functions that enable the ability to manage and react to change. Real-time data should enable accurate reporting and it is important that the design of application whitelisting technology be configured in such a way as to allow for easy visibility into the reporting tools it has to offer.

Moving Forward with Application Whitelisting

The discovery of the Stuxnet worm in 2010 brought the potential of cyber attacks to the attention of the industrial control system community like no other previous event. 2011 was the year that most organizations demonstrated their readiness to develop and deploy cyber tools as a result of the highly publicized Stuxnet attack. However, other cyber weapons, used to destroy data at any given time, are likely to be more widely used. Programs such as kill switches, logic bombs, and other threats can be developed on a regular basis and deployed systematically.

The challenge for industrial control system managers is one of preparation, vigilance, and agility. Part of that preparation is utilizing tools to prevent potential attacks while applying them as part of a broader security strategy. Application whitelisting is one tool that should be used as a complementary security defense. While it does detect attacks that other technologies don't, threats like buffer overflows, SQL injection and cross-site scripting are better controlled when combined with well suited tools like antivirus programs.

Regardless of the depth of initial usage in control systems, whitelisting is a technology that can provide another layer of defense in protecting industrial process control systems.

[1] McAfee Threats Report: First Quarter 2012. Page 6 http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2012.pdf

For More Information
Learn more about how Honeywell’s Industrial Cyber Security Solutions and how they can enhance the security of your operations, visit our website www.becybersecure.com or contact your Honeywell account manager.

Honeywell Process Solutions
Honeywell
1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG121EB

Shanghai City Centre, 100 Junyi Road
Shanghai, China 20051

www.honeywellprocess.com

WP-12-26-ENG
October 2012

Honeywell