ELECTRIC POWER
RESEARCH INSTITUTE

Guidelines for Deploying Application Whitelisting

3002003919

Guidelines for Deploying Application Whitelisting

3002003919

Technical Update, May 2018

EPRI Project Manager

G. Chason

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE ELECTRIC POWER RESEARCH INSTITUTE (EPRI) PREPARED THIS REPORT.

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

Copyright © 2018 Electric Power Research Institute, Inc. All rights reserved.

ACKNOWLEDGMENTS

The Electric Power Research Institute (EPRI) prepared this report.

Principal Investigator
G. Chason

This report describes research sponsored by EPRI.

This publication is a corporate document that should be cited in the literature in the following manner:

Guidelines for Deploying Application Whitelisting. EPRI, Palo Alto, CA: 2018. 3002003919.

ABSTRACT

Application whitelisting (AWL) technologies have evolved from their early beginnings as a simple protection mechanism preventing unauthorized software applications from running on a system. Traditional AWL was, as the name implies, a list of software applications approved for loading into memory and permission to run on a target central processing unit (CPU). AWL as a solution is intended to limit operations to known good applications, thereby limiting the scope of work needed to be performed by entities responsible for system security. For basic Energy Management Systems (EMS) this task is as well defined as the systems it is implemented to protect. However, as malevolent actors in system environments have increased their capabilities, AWLs have been adapted. Changes in the complexity of protected systems has also required AWL solutions to increase their capabilities and adaptability to remain viable solutions.

The deployment of application whitelisting solutions in environments with multiple platforms hosting multiple vendors with a wide range of requirements, such as most EMSs, can be resource intensive (equipment, network infrastructure, and personnel). This type of deployment is further complicated by the diversity of implementations for policy, mode, and denial enforcement. It is further noted that host system requirements are highly variable and that many of the more robust AWL solutions are tightly tied to other functionality within multi-purpose products.

Any organization considering the deployment of one or more AWL solutions should engage impartial subject matter experts (SMEs) having experience, and a thorough understanding of, AWL and the target deployment environment. This team should perform a thorough analysis of the target system(s) as deployed and a thorough analysis of the solution(s) being considered for deployment. With these analyses being complete, the team should then perform both a risk analysis and threat analysis for the deployed AWL(s) as they would be deployed in the target system(s).

Keywords
Application whitelisting
Cyber security
Energy management systems

Deliverable Number: 3002003919

Product Type: Technical Update

Product Title: Guidelines for Deploying Application Whitelisting

---

PRIMARY AUDIENCE: Utility personnel responsible for cyber security of control centers and energy management systems.

SECONDARY AUDIENCE: Utility personnel responsible for the management of energy delivery systems.

KEY RESEARCH QUESTION

The focus of the research reported in this technical update is the utility of deploying application whitelisting (AWL) with energy management system (EMS) deployments. The goal is to identify guidance on the identification, selection, and deployment of application whitelisting solutions as a security mechanism for an EMS.

RESEARCH OVERVIEW

The research reported in this technical update focused on two primary areas. The first is the identification of application whitelisting solutions suitable for deployment as part of a framework providing cyber security for an EMS. The first area considered was the degree to which use of the AWL may represent additional overhead for utility personnel. The second area was guidance on the selection and evaluation of AWL solutions.

KEY FINDINGS

- Traditional AWL solutions provide increased cyber security, but are not a panacea.
- Most commercial AWL solutions available today are bundled with non-AWL functionality / systems; adding complexity, time, and cost to the deployment of whitelisting capabilities.
- AWL solutions are not without vulnerabilities of their own.
- Consistency across solutions from different vendors and deployments is highly variable.
- Deployment of stand-alone AWL solutions on systems with very well defined and focused operations can provide significant protections when the enforcement mechanisms are well understood and well managed by the deploying organization.

WHY THIS MATTERS

The research results provided here give an overview of issues that should be considered prior to AWL solution selection. Guidance includes points of consideration for the gauging the benefits and costs (time and resources) associated with AWL deployment and operations.

HOW TO APPLY RESULTS

Guidance provided should first be reviewed with organizations responsible for procurement, deployment, utilization, and maintenance of AWL solutions for the target EMS. This review should include in-depth analysis focused on the benefits and costs for the deploying organization. With this analysis, the deploying organization can engage prospective solution vendors to obtain a greater depth of understanding for the solution's potential to increase cyber security for the EMS at an acceptable cost (time and resources).

EPRI CONTACTS: Project Manager: Glen Chason, Principal Technical Leader, gchason@epri.com.

PROGRAM: Cyber Security program P183.

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

© 2017 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER...SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

ACRONYMS

This section provides acronyms for key terms used in this report.

AWL Application Whitelisting

CPU Central Processing Unit

DLL Dynamically Linked Library

EMS Energy Management System

IP Internet Protocol

RFP Request For Proposal

SME Subject Matter Experts

CONTENTS

ABSTRACT ..... **V**

EXECUTIVE SUMMARY ..... **VII**

ACRONYMS ..... **IX**

***1* OVERVIEW** **1-1**

Execution Policies 1-1

Default Denial 1-1

Detect-and-Deny 1-1

Detonate-and-Deny 1-2

Operating Modes 1-2

Learning Mode 1-2

Protection Mode 1-2

Alert Mode 1-3

Traditional File Validation and Enforcement 1-3

Attributes 1-3

Hashing 1-3

Trusted Publisher 1-3

Dynamic Forms of File Validation and Enforcement 1-4

Reputation 1-4

Detonation 1-4

Term Overloading 1-4

***2* GUIDANCE** **2-1**

Recommendations 2-1

Operating Modes 2-1

Enforcement Mechanisms 2-2

System Considerations 2-3

***3* CONCLUSIONS** **3-1**

***4* REFERENCES** **4-1**

***A* VENDORS** **A-1**

Whitelisting Products A-1

LIST OF TABLES

Table A-1 Example Solution Providers Overview A-1

1
OVERVIEW

Application whitelisting (AWL) technologies have evolved from their early beginnings as a simple protection mechanism preventing unauthorized software applications from running on a system. Traditional AWL was, as the name implies, a list of software applications approved for loading into memory and permission to run on a target central processing unit (CPU). AWL as a solution is intended to limit operations to known good applications, thereby limiting the scope of work needed to be performed by entities responsible for system security. For basic Energy Management Systems (EMS) this task is as well defined as the systems it is implemented to protect. However, as malevolent actors in system environments have increased their capabilities, AWLs have been adapted. Changes in the complexity of protected systems has also required AWL solutions to increase their capabilities and adaptability to remain viable solutions. One area in which adaptations have occurred is execution policies.

Execution Policies

Default Denial

In its purest form, whitelisting operations initially deny all software applications (note that this does not include the operating system hosting the whitelisting solution or the whitelisting solution itself) access to a protected CPU. Access is granted only when the whitelisting solution has approved the target application software. If the software requesting processor access is not in the list, access to the CPU, also known as processor context, is denied by default.

In its simplest form, “Default-Deny” implementations simply rely upon an applications name, such as it may be registered with the host operating system, or otherwise identified to the AWL solution by an administrator. However, this simple form is highly susceptible to spoofing or masquerading attacks and rarely found in existing AWL solution. Moving beyond this most simple form, more robust mechanisms have been developed to provide increased authentication and integrity validation of executables. However, these mechanisms still rely upon the static criteria established when the whitelist is created or updated by an administrator. Additional information on advances in application identification, authentication, and integrity validation are provided below under the section titled: **Operating Modes**.

As with changes in application identification, the denial of context is no longer limited to traditional applications. Depending upon the AWL solution, other executables (dynamically linked libraries (DLLs), processes, threads, etc.) may be denied context if not specifically allowed by policy or explicit inclusion in the whitelist. Therefore, use of default-deny policies may require each executable to be in the whitelist prior to the request for context.

Detect-and-Deny

In contrast to the static nature of default-deny policies, detect-and-deny policies provide for the granting of context to an application or executable based upon verification of reputation,

typically provided by a service[1]. There are numerous mechanisms by which reputation can be verified. These mechanisms range from local repositories to databases that collect reputation information world-wide. The more expansive mechanisms may utilize information from the vendor and/or third parties. Use of this policy is less restrictive than default-deny since the rational for granting context to an application is based upon factors not associated with the content of the binary file requesting context.

Detonate-and-Deny

Detonate-and-deny, also known as verify-and-deny, is used to send files (executable and non-executable) from endpoints to detonation services for evaluation of suspicious content and in the case of executables, context approval. This policy type can be used more effectively in environments where executable content may be added at irregular intervals. This would include environments where removable media is required, allowing new media content to be evaluated as it is presented to the system for execution. This policy type can also be used for occasions when devices need to be vetted after being temporarily off-line. In such cases, reconnecting to the host system results in files being sent to the host system for evaluation. This policy provides additional protections for devices operating in hard to access or remote locations.

Operating Modes

Learning Mode

Learning mode is a feature of some whitelisting solutions. Where learning mode is employed, the whitelisting solution monitors the host system for file execution. When a file is granted context, the solution identifies the file and places it into a temporary whitelist. Most supporting solutions provide users an option to review and accept the list prior to implementing the whitelist as part of the protection mode. The review phase is a critical component when learning mode is used due to the potential for malicious binaries to be executing during the learning phase.

Protection Mode

Protection mode is the normal operating mode for protections provided by whitelisting solutions. In this mode, the whitelist is used in accordance with the policies (as supported by the vendor solutions) described under Execution Policies above.

Mode Variants

In addition to general learning and protection modes, many solutions providers offer variants of both. For example, an older solution called Parity, from Bit9 (now a part of Carbon Black) supported a type of learning mode in which all requests were granted context and the access was logged for later review. Another variant of the learning mode was the use of the identification of requests for binaries for which whitelist approval had not yet been granted. In this mode, the administrators were queried when previously unlisted software requested context, allowing the administrator to allow the execution.

---

[1] Software reputation services, NIST 800-167, page 6 [1].

Alert Mode

Some AWL solutions offer an alert mode. In this mode, the AWL solution does not block an executable from running when it is not found in the whitelist. Instead of blocking, the AWL provides the executable a context allowing it to run, but also sends an alert to the users informing them that a non-whitelisted executable has been allowed to run. This mode does not provide true protection, but may be an acceptable alternative to blocking in situations where unintended block can negatively impact system operations.

Traditional File Validation and Enforcement

There are several forms of whitelisting file validation that have traditionally been used. These traditional forms are based upon characteristics, evaluated prior to granting context to the executable code.

Attributes

Attributes upon which evaluation of execution privilege can be based, take several forms. One form is file attributes. This form utilizes characteristics of the file containing the executable code and includes attributes such as file name, size, updater, owner, and location. These forms of attributes are generally considered weak as they can be easily manipulated by an adversary with administrative access. For example, an adversary with administrative access could place a malicious file in any file path hierarchy that had execution privileges. These privileges would allow the malicious code to execute as any file in the hierarchy would have this privilege. Similarly, whitelisting executables by name is very weak as an adversary with administrative privileges could overwrite a valid file with malicious content.

Hashing

Hashing operations are used to generate a message digest representative of the executable on which the hashing operation was performed. This digest is a one-way cryptographic mechanism used to validate the integrity of the executable. To perform the validation, the receiver executes the hash over the received file and then compares the hash generated to the hash received from the publisher. If the hashes match, the integrity of the executable is validated. Hashing alone can be used for integrity validation, but does not provide a mechanism for authentication.

Trusted Publisher

Trusted publishers typically utilize a form of digital signature to “sign” their respective executable software. The signature is created when the publisher generates a message digest for the executable to be signed. The message digest is then encrypted with the publisher’s private key and the encrypted message digest is made available to the recipient of the executable. Upon receipt of the executable and encrypted message digest the receiver regenerates the message digest over the received executable. The result is then compared to the decrypted message digest received from the publisher, using the publisher’s public key, and the two message digests are compared. If they match, the integrity and authenticity of the executable is considered to be verified.

Dynamic Forms of File Validation and Enforcement

There have been advancements in the file validation and enforcement mechanisms utilized by application whitelisting solutions. These non-traditional forms utilize factors and methods that are not derived directly from the file being validated.

Reputation

More recent developments in AWL technology include the use of reputation services. These services, provided by the AWL vendor or a third party, are queried when an executable is identified for execution. The service provides an assessment of the executable based upon known information available about the executable. The methodologies of gathering and assessing data varies significantly between services. Utilization of service provided reputations also varies widely by vendor and should be reviewed thoroughly to ensure access or loss of access does not violate compliance requirements or negatively impact operations of the system for which the AWL provides security operations.

Detonation

Detonation utilizes the running of the executable in a sandbox environment to evaluate its behavior. If the executable is determined to be safe, it is provided a context and allowed to run on the target system. The criteria for determining if the file is "safe" varies significantly by AWL provider. Criteria that has been identified as useful by one or more providers include:

1. Memory addresses accessed
2. Interactions with other executable files
3. Communications
    a. Attempts to access remote locations
    b. Attempts to exploit other executables
4. Identification of embedded malware (by signature or behavior)

Implantation of detonation functionality may be provided by the AWL or may utilize the services of another device. For example, network equipment providers such as Palo Alto and FireEye provide detonation services for executable files identified as they transit the network infrastructure[2].

Term Overloading

When evaluating AWL solutions, notice should be taken of overloading the term "whitelisting". Many cyber security and non-security related functions and features use "whitelists" when describing certain operations. For example, the term whitelist can be used to identify a set of ports or internet protocol (IP) addresses which are allowed access through a firewall. The whitelist contains the list of accessible ports. Similarly, some products provided users with the ability to whitelist operational features while blacklisting others. Because of terminology overloading, AWL selection and evaluation processes and discussions need to ensure that clear and accurate terminology is used.

---

[2] CarbonBlack provides additional information in their paper on Cracking Energy and Utilities [].

2
GUIDANCE

Initial guidance, at project inception, for the research performed focused on application whitelisting for Energy Management Systems (EMSs). However, through initial findings and discussions with project advisors, it was determined that a broader scope would better serve the needs of the advising electric sector utilities.

For systems that are tightly structured and change very rarely, management of the list for default-deny AWL operations can be straight forward and require minimal maintenance. However, it should be noted that **ALL** aspects of system operations, including failure scenarios, be evaluated for executables that may need to exercise rarely used functionality. In addition to the frequency of execution, AWL solutions should be vetted for how the AWL determines if an executable is denied context. More information on the various forms of whitelisting impacting execution selection can be found in the section on **Operating Modes** below.

Recommendations

This section contains recommendations developed during this research and derived, and credited, directly from other sources. Recommendations are included here to facilitate the knowledge transfer and do not correspond to identifiers in other originating sources. In addition to these specific recommendations, the Homeland Security "Application Whitelisting (AWL): Strategic Planning Guide" [4] provides additional guidance. It is recommended that the strategic planning guide be reviewed in conjunction with this report and that Appendix A of the guide be reviewed prior to requests for proposals (RFPs) or other procurement activities.

Operating Modes

Learning mode

5. Learning mode should be used a first step to deployment. This will allow system operators to gauge initial impacts of whitelisting operations to the EMS.
6. Learning mode can be used for system analysis to validate the executables running on the system. This provides system operators an opportunity to identify execution of unexpected code without the potential negative impacts of running the AWL in protection mode.
7. If available, a stand-alone AWL capable of running learning, protection, and alert modes provides a significant advantage in the deployment sequence. Initial deployment would be in learning mode, and the initial whitelist developed from the results of learning operations. The deployment team could next use the AWL in alert mode for some trial period to identify potential anomalous conditions without negatively impacting operations. If after the alerting mode trial period, concerns remain regarding potential negative impacts when protection mode is engaged, the deploying organization can continue running in alerting mode. This does not provide the same protections as protection mode, but may increase situational awareness of malicious activities.

4. Where feasible, deploying organizations should ensure that as many operational scenarios as possible are executed while the system is in learning mode. Where practical, known events, adverse events, and incidents[3] should be recreated to determine the AWL's response to those and similar occurrences.

Enforcement Mechanisms

Attributes

1. Use of attributes such as trusted path and file name are considered weak and it is recommended that they not be used.

Hashing

1. Hashing alone is not recommended for use in establishing trust for a published executable. For solutions that utilize hashing without authentication, other run-time safeguards need to be in place to protect against, or at a minimum detect file changes.

Trusted Publishers

1. The cryptographic methods supported by an AWL solution in establishing publisher trust should be identified and vetted against NIST approved algorithms [2].
2. The methods for exchanging information used to validate publisher trust should be vetted. This vetting should include the algorithms used and the infrastructure/processes through which the information must flow prior to being used by the host systems deploying the target application.
3. An analysis of the mechanisms used and requirements for trust revocation should be performed for each solution irrespective of vendor.

Reputation

1. When reputation is an available option for execution control enforcement, a review of the methodologies for reputation creation, updates, distribution, and utilization should be conducted. This review should include, at a minimum:
   a. How is the information upon which the reputation is based is collected and analyzed?
   b. How is the reputation scored and how often the scores are updated?
   c. What are the means of reputation distribution to the AWL and the refresh rate for the scored reputation?
   d. How is the score used by the system?
      i. Is the score retrieved each time execution is requested?
      ii. If not retried each time, how is the reputation re-used?
   e. Is there an expiration on the reputation if not updated upon each execution request?
   f. How does AWL respond if the reputation is expired or not recoverable from the service?

---

[3] Section 2.1 of NIST SP800-61 [3]

Detonation

1. What are the criteria by which executable detonation is executed?
2. Where is the detonation evaluation conducted?
   a. In the AWL?
   b. By utility owned third party equipment?
   c. By a remote service?
3. What indicators are provided when an executable is detonated and refused a context?
   a. What information is provided by the AWL?
   b. Are third parties notified of the detonation?

System Considerations

In addition to considerations for the AWL, other EMS security components need to be taken into account when evaluating the use of AWL for the EMS. These considerations should include holistic considerations for deployed software and network security measures. Several sample questions are provided below to serve as example considerations. However, this list should not be considered either complete or comprehensive as the scope of considerations will vary significantly across deployments.

1. Will remote access be required by the AWL?
2. How will the need for remote access affect the placement of the AWL?
   a. Would the use of remote access, considering a recommended placement, negatively impact compliance or increase workload to maintain compliance?
   b. Will organizations, other than the deploying organization, be required to make changes to their security systems? Examples would include changes to firewall settings, equipment updates (perhaps supporting network detitanation), additional servers, etc.
3. Will the AWL be implemented with existing security measures such as anti-virus?
4. Will any existing system operations execute outside the AWL? Examples may include operations such as intrusion detection, intrusion prevention, and software used to test other security measures?
5. Are there operational situations during which the AWL will need to be disabled in order to prevent erroneous reporting?
6. To what extent might AWL operations impact processor utilization or network throughput?

3
CONCLUSIONS

The basic concepts associated with application whitelisting are well understood and have proven potential to improve cyber security for the host platform. However, the deployment of application whitelisting solutions in environments with multiple platforms hosting multiple vendors with a wide range of requirements, such as most EMSs, can be resource intensive (equipment, network infrastructure, and personnel). This type of deployment is further complicated by the diversity of implementations for policy, mode, and denial enforcement. It is further noted that host system requirements are highly variable and that many of the more robust AWL solutions are tightly tied to other functionality within multi-purpose products.

It is recommended that any organization considering the deployment of one or more AWL solutions engage impartial subject matter experts (SMEs) having experience and a thorough understanding of AWL and the target deployment environment. This team should perform a thorough analysis of the target system(s) as deployed and a thorough analysis of the solution(s) being considered for deployment. With these analyses being complete, the team should then perform both a risk analysis and threat analysis for the deployed AWL(s) as they would be deployed in the target system(s).

4
REFERENCES

1. NIST Special Publications (SP) 800-167, October 2015, Guide to Application Whitelisting, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-167.pdf
2. NIST Computer Security Resource Center, https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/validation
3. NIST Special Publications (SP) 800-61, Revision 2, August 2012, Computer Security Incident Handling Guide https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
4. Department of Homeland Security "Application Whitelisting (AWL): Strategic Planning Guide", https://www.us-cert.gov/sites/default/files/cdm_files/FNR_NIS_OTH_AWL_Strategic_Planning_Guide.pdf
5. Department of Homeland Security "Guidelines for Application Whitelisting In Industrial Control Systems", https://ics-cert.us-cert.gov/sites/default/files/documents/Guidelines%20for%20Application%20Whitelisting%20in%20Industrial%20Control%20Systems_S508C.pdf
6. Carbon Black, "Cracking Energy and Utilities: Inter Tips for Endpoint Security", https://www.carbonblack.com/wp-content/uploads/2017/04/2016_cb_eb_cracking_energy_utilities.pdf

A
VENDORS

This appendix is provided for reference and represents resources that were used in the development of this report. This report does not endorse or in any way advocate any one vendor or solution. This list is provided for reference purposes only.

Whitelisting Products

Numerous commercial products exist for implementing whitelisting solutions. The degree to which any product may be applicable for deployment within an EMS environment is highly dependent upon the deploying utility's architecture(s) and vendor choices. Table A-1 provides a sampling of vendors with available solutions that may be applicable to an EMS deployment. However, as was noted in text above, AWL functionality is often packaged with non-AWL functionality. This point should be addressed when discussing AWL with solution providers. The cross section presented in Table A-1 should not be considered as comprehensive, nor should inclusion of a vendor solution in the table be construed or considered as an endorsement of the solution.

Table A-1
Example Solution Providers Overview

AppLocker	
Solution Provider	Microsoft[4]
Underlying Technology Source	Provider developed
Supported Policies	Default-Deny
Supported Operating Systems	Windows Server Windows 7, 8, and 10
Supported File Types[5]	Windows Executables (.exe) Dynamically Linked Libraries (DLLs) Scripts Windows Installers Packaged Applications and Installers
Validation Database Support Options	NA
Available Application Approval Mechanisms	Trusted Publishers Attributes File Hash
Known / Previous Vulnerabilities[6]	CVE – 2011 - 4434

[4] https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/how-applocker-works-techref

[5] Separate rule set for each of the file types.

Table A-1 (continued)
Example Solution Providers Overview

Cb Protection	
Solution Provider	Carbon Black[7] - Carbon Black was purchased by Bit9 in 2014 Bit9 was rebranded to Carbon Black in 2016
Underlying Technology Source	Provider developed and Bit9
Supported Policies	Default-Deny Detect-and-Deny Detonate-and-Deny
Supported Operating Systems	Microsoft Windows MacOS Red Hat Linux CentOS
Supported File Types[5]	Broad range[8]
Validation Database Support Options	On-Site Cloud Based
Available Application Approval Mechanisms	Trusted Publishers Attributes Reputation Detonation Metadata
Known / Previous Vulnerabilities[6]	CVE – 2016 - 9570

[6] Vulnerabilities identified are not representative of current software, but are provided as indication that potential vulnerabilities need to be researched for solutions under consideration for procurement.

[7] Cb Protection: https://cdn.www.carbonblack.com/wp-content/uploads/2017/04/CB_Protection_DS_040618.pdf

[8] Support for Detect-and-Deny provides support for a much broader range of file types.

Table A-1 (continued)
Example Solution Providers Overview

Exe-Guard	
Solution Provider	Schweitzer Engineering Laboratories (SEL)
Underlying Technology Source	Provider developed
Supported Policies	Default-Deny
Supported Operating Systems	Embedded Linux
Supported File Types[5]	Broad range[8]
Validation Database Support Options	On-Site
Available Application Approval Mechanisms	Trusted Publishers
Known / Previous Vulnerabilities[6]	CVE-2017-7928
Experion PKS Application Whitelisting Industrial Cyber Security Risk Manager	
Solution Provider	Honeywell
Underlying Technology Source	Provider developed and Bit9
Supported Policies	Default-Deny Detect-and-Deny
Supported Operating Systems	NA
Supported File Types[5]	Broad range[8]
Validation Database Support Options	NA
Available Application Approval Mechanisms	NA
Known / Previous Vulnerabilities[6]	CVE – 2016 - 8344 ICS Cert - Advisory (ICSA-14-352-01) ICS Cert - Advisory (ICSA-15-272-01)

Table A-1 (continued)
Example Solution Providers Overview

Managed Application Control	
Solution Provider	Trustwave
Underlying Technology Source	Proprietary
Supported Policies	Default-Deny Detect-and-Deny Detonate-and-Deny
Supported Operating Systems	Microsoft Windows MacOS Red Hat Linux CentOS
Supported File Types[5]	Broad range[8]
Validation Database Support Options	NA
Available Application Approval Mechanisms	NA
Known / Previous Vulnerabilities[6]	NA
Workspace Manager – Endpoint Security – Application Control	
Solution Provider	Ivanti – Heat Software was purchased by Ivanti in 2017 Lumension merged with Frontrange in 2015 to form Heat Software CoreTrace was purchased by Lumension in 2012
Underlying Technology Source	Provider developed, Lumension, and CoreTrace
Supported Policies	Default-Deny Detect-and-Deny
Supported Operating Systems	Microsoft Windows Linux MacOS
Supported File Types[5]	Broad range[8]
Validation Database Support Options	Cloud-based
Available Application Approval Mechanisms	Trusted Publishers
Known / Previous Vulnerabilities[6]	CVE – 2017 - 11463 CVE – 2018 - 6316

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI members represent 90% of the electric utility revenue in the United States with international participation in 35 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

© 2017 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

3002003919

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com