Homeland Security

Federal Network Resilience

APPLICATION WHITELISTING (AWL) READINESS QUESTIONNAIRE

Background and Purpose

Application Whitelisting (AWL) is considered one of the top ways to mitigate risk from cyber attacks. It is the number 1 recommendation in NSA IAD's Top 10 Mitigation Strategies[1], one of the Australian Defence Signals Directorate Essential 4 in their Strategies to Mitigate Targeted Cyber Intrusions[2], and part of the Council on CyberSecurity's First Five in their 20 Critical Security Controls[3]. It seems that the extended security community has come to a consensus that AWL is one of the most important security technologies/techniques an organization can and should implement.

If everyone agrees it is the right and one of the best things to do, then why do so few organizations have a viable working implementation? There are plenty of commercial tools and vendors that advertise their ability to perform AWL. A few of the products in widespread use have built-in AWL capabilities, and there are plenty of informative and easy to understand guidance documents on how to use those capabilities. Still most CISOs and their staff cringe at the thought of implementing AWL. They believe it to be "impossible" or "suicide" for their organization. There are a fair number of stories about failed implementations and very few about successful ones.

It appears that there are some key factors that need to be in place for an organization to implement an effective and sustainable AWL solution. This questionnaire is designed to help an organization determine if they are ready ***to start*** the process of planning for an AWL implementation. While most organizations analyze technical readiness prior to making a deployment decision, it turns out that AWL solutions also require a level of cultural and process readiness. Until the following conditions exist, the likelihood of deploying a successful AWL implementation is low.

By using the content and questions within this document, organizations can begin defining what processes and policies need to be in place and how to execute them to support a successful AWL program.

[1] http://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_Top10IAMitigationStrategies_Web.pdf
[2] http://www.asd.gov.au/infosec/top-mitigations/mitigations-2014-table.htm
[3] https://www.sans.org/critical-security-controls

Keys to Success

Organizations usually jump to tools and technologies when creating an implementation plan for deployment of a security-related capability. In the case of AWL, the factors that lead to success are often less about technology and more about existing culture and processes. The 3 most critical elements of a successful AWL deployment are:

1. **Visible Management Support** at all levels of the organization
2. The ability to **Communicate Early and Often** with users, IT support staff, and mission leaders
3. Spend the time to understand your environment, needs, and options to **Develop a Plan that Fits Your Organization**

Readiness Questions

An organization does not need to answer "yes" to every question to be able to plan and implement a successful AWL program. An organization must be willing to openly communicate support for, and enforce the actions necessary to address, these questions. For example, it is possible that the organization currently supports a large number of people with administrator or software installation privileges. In this case, a successful AWL program will require individuals in key management positions to openly and vocally support the IT and security staff in enforcing new rules for who can install software. They can do this by notifying the workforce of the need to change the existing policies and fully supporting IT/security personnel during disputes or requests for exceptions. The willingness of managers to take these actions is more important than whether or not the current environment restricts privileges.

Cultural Readiness

For AWL solutions to work, you need to restrict what software can be installed, who can install it, and where it can be installed. This takes a level of discipline that must be enforced across the ***entire*** organization. It also means that you will be telling individuals and mission organizations that they can no longer behave in the manner to which they have become accustomed. For example, not everyone will have the right to install software, and not all software that individuals currently find useful or convenient will be allowed. Initialization and sustainment of the AWL solution will take resources, at times requiring high value individuals who have a solid understanding of both technology and mission. Basically, there will be complaints, requests to be excluded from the solution, and competition for already limited resources. Your entire organization – from top to bottom - must see AWL as a core mission requirement, not as a

mandated security feature that restricts the mission.

Management Engagement

Management support is essential, but not sufficient for successful implementation. There needs to be vocal and visible support for the AWL solution at all levels. Everyone has seen instances where leadership sends out an email stating that something is important, but then makes operational decisions that run counter to that assertion. The organization has to undergo a cultural shift to accept the discipline and new operational realities that come with AWL solutions, and cultural shift requires active committed leadership.

There will probably be pressure for AWL decision makers to provide exceptions for individuals and organizations that believe they should not have to be bound by the new policies. It is important to protect these decision makers by making sure that key management personnel will support them in these disputes and prevent unhappy users from "jumping" the chain of command to get policies or decisions changed.

- ***Do the senior leaders see the value of AWL to the mission?***
- ***Are they willing to commit the necessary resources and make the AWL implementation a high priority?***
- ***Are they willing to back the AWL program in disputes that are based on perception and a desire to maintain the status quo, and not true mission impact?***
- ***Are they willing to engage the workforce on an ongoing basis to express the importance of AWL and their commitment to the program?***

Discipline as a Core Tenet

As stated earlier, AWL solutions require organizations to establish and enforce a level of discipline with respect to software installation that is rarely the norm. The best AWL implementation cannot provide the security it is designed to provide if everyone has administrator privileges. Implementation and maintenance become resource intensive and have an increased potential to impact mission if every organization can ***at will*** decide what software can be installed and where it can be installed.

- ***Does your organization limit who has administrator privileges? Is it willing to?***
- ***Does your organization define and enforce software installation policies across the entire enterprise? Is it willing to? What about the organizations that have reciprocal rights in your enterprise (e.g., windows trust relationships)?***
- ***If there are certain groups that are allowed to make their own policies or manage their own systems: Are they held accountable to any baseline standards of behavior? Are***

they under the direction of senior leadership that supports restricting who can install software and where it can be installed?

Communication Options

Communications are critical to a successful AWL implementation. There seems to be a large amount of fear, much of it based on a perception of AWL, and working at all levels to involve and share information with all employees is one of the only ways to dispel this fear. There needs to be ongoing communication between management, IT professionals, and system users. This communication cannot be just one way statements or assertions. Users and mission managers need to feel heard. IT professionals from different organizations need to work together to establish and enforce a viable policy and timely resolution process for issues. Management needs to stress the importance and value of the AWL program through words and actions.

- ***Does your organization have multiple mechanisms for communicating with the workforce? Does it have well established ways to collect workforce comments and concerns?***
- ***Does your organization have established mechanisms for IT staff from different parts of the organization to collaborate, including remote participation?***
- ***Is your leadership willing to share information with the workforce on an ongoing basis? Is the IT leadership willing to do the same?***

Process Readiness

The next level of readiness is to make sure you have processes in place that support AWL implementation planning and associated decisions. There are many ways to stage an AWL implementation such that you can incrementally improve your ability to protect critical mission information while minimizing operational impact. To do that, you need to know enough to decide on an appropriate implementation strategy; work with existing processes to gather important information required for operation; and have a way to incrementally upgrade (or rollback) the solution for different parts of your enterprise at different times.

Knowing Your Environment

As previously stated, there are many ways to incrementally deploy an AWL implementation. Developing a strategy that most appropriately balances security, mission, and resources requires knowing something about numbers, locations, criticality, technology, and support mechanisms for mission information, applications, servers, and devices. It also involves understanding the existing processes for change management, deployment, and maintenance of software to

identify and address standardization, automation, and timeliness issues.

- ***Does your organization have existing processes for maintaining a reasonably accurate hardware inventory?***
- ***Does your organization have existing processes for maintaining a reasonably accurate software inventory for the enterprise? Does it have a view of what operating systems and applications are installed on which pieces of hardware (to include what versions)? Does it know the general number of applications that will need to be whitelisted?***
- ***Does your organization have a reasonable understanding of specialized mission and network applications? Does it know where they are used, how they are used, and the operational requirements that affect software installation and management?***
- ***Does your organization have an existing view of what hardware and applications are associated with what missions? Does it have some view of mission criticality for the assets in the above inventories?***

Feeding the Solution

Regardless of which solution or implementation strategy you select, there is information that must exist and be provided to the AWL program in a routine and timely manner. This includes, but is not limited to, information on authorized software and operational installations of that software.

- ***Does your organization have a process for authorizing software for use in the environment? Is this process timely and used across the organization? Does it have a mechanism for sharing this information and the software, such that the AWL implementation can be updated in a timely and seamless manner?***
- ***Does your organization have a standardized process or approach to distributing and installing authorized software? How can this process be augmented to ensure that newly deployed software is already accounted for in the AWL solution?***
- ***Does your organization have a process or set of processes for managing images deployed in the operational environment? Does it have a mechanism for sharing those images such that the AWL implementation can be updated in a timely and seamless manner?***

Managing the Implementation

Effective and appropriate AWL implementations are deployed incrementally across the enterprise. They are trained on the existing environment and alerting is enabled prior to any blocking or prevention policies are enforced. They start with simpler AWL techniques and evolve to the complex process of defining and restricting executables based on hash or software product manifest. There are

many dimensions of an AWL solution to manage, and they can be implemented in a different manner or at different times for different parts of the organization. Therefore the organization needs to be able to support a flexible and responsive implementation strategy.

- ***Does the organization have experience planning and executing incremental deployments?***
- ***Does the organization have processes, mechanisms, and the necessary resources to implement and maintain an incremental deployment?***
- ***Are the processes flexible and timely enough to support modifications to a deployment triggered by operational conditions?***
- ***Are the processes flexible and timely enough to support near-real-time rollback to a previous state of a deployment?***

Technical Readiness

There is a fair amount of conflicting information about how easy or hard it is to implement AWL solutions, what types of resources are required, and what types of deployment strategies are most successful. Therefore we offer a minimal set of items that you could use to determine if certain solutions and strategies are appropriate for your organization prior to starting the planning process.

Tools and Techniques

- ***Does your organization have a perspective on what AWL methodology4 is desired or appropriate?***
- ***Does your organization plan on purchasing a commercial tool to perform AWL? Does it already purchase technologies or services that support AWL functions?***

Resources

- ***Does your organization have resources with the appropriate skills to support the different stages of an AWL implementation?***
- ***Are those resources supporting other high priority activities? Is there a process for requesting and/or receiving their support?***
- ***What are the resource constraints that will have to be applied to the AWL program?***

[4] The main AWL methodologies are location-, certificate-, reputation-, behavior-, and hash-based whitelisting. See companion document *Application Whitelisting (AWL): Strategic Planning Guide* for more information on the methodologies.

Deployment Options

- ***What processes are used by your organization to roll out technology upgrades? What is the current schedule for planned upgrades? Is it too late to "piggy back" on those upgrades as part of the AWL deployment?***
- ***Does the AWL program have the necessary contacts in the other IT support organizations to understand localized planned upgrades and/or deployment processes?***