Application Whitelisting Buyer's Guide

NYOTRON
SECURING THE WORLD

What is Application Whitelisting (aka Application Control)?

One approach to combating viruses and malware is to whitelist any software application which is considered safe to run, and block all others (SANS Institute).

This default-deny or zero-trust approach has a number of benefits. The US Government, including the intelligence community, is a strong supporter of whitelisting. The National Institute of Standards and Technology (NIST) states, "Application whitelisting solutions are generally strongly recommended for hosts in high-risk environments where security outweighs unrestricted functionality."

> *"... application whitelisting is the most effective way to significantly reduce the impact of malware in today's environments."*
>
> **– The SANS Institute**

In summary, application control technologies allow security pros to limit the applications that can run in their environment. Ostensibly this form of whitelisting reduces the surface of attack by limiting available options exploited by a would-be perpetrator.

Potential Pitfalls

The management overhead of application whitelisting can be a significant burden in many environments. The number of applications can easily rise into the millions (so too does the number of malware variants), and today's knowledge workers with a broad range of responsibilities require a diverse and an ever-evolving set of applications to perform their roles. Manually updating and managing whitelists inevitably demands an incredible amount of time and energy these workers don't have to spare. To make matters more complicated, the use of fileless malware and the so-called Living off the Land (LotL) tactics that use legitimate administrative tools often included with the operating system, are becoming more prevalent. Attackers leverage these tactics to bypass application whitelisting as well as many other security tools. Even Symantec cautions that "Pure application whitelisting will not prevent the misuse of dual-use tools." (Symantec)

Organizations must also contend with zero-day attacks that exploit a software vulnerability that was previously unknown or undisclosed by the software vendor. Whitelisting may not protect an organization if the vulnerability exploited is within an approved (whitelisted) application. Vulnerabilities within web browsers, Java, Adobe and Microsoft Office applications are very common. There are very few environments where these applications are not whitelisted.

Evaluating Application Whitelisting Solutions

> *"... properly configured AWL [Application Whitelisting] should be an integral component of a defense-in-depth solution."*
>
> **– National Cybersecurity Communications and Integration Center**

In today's threat environment, the use of a zero-trust approach like whitelisting in an organization's endpoint and server protection toolkit is essential. However, it is important to thoroughly evaluate solutions available on the market to pick the right one that suits your specific needs and requirements.

Use this questionnaire when evaluating any vendor's whitelisting or similar solution:

Question	Vendor A	Vendor B
Does the product protect from the following types of attacks?		
Ransomware attacks		
MBR attacks (e.g. wiper malware)		
File-less/in-memory attacks (e.g. DLL hijacking)		
Script-based attacks (e.g. MS Office macros)		
"Living off the land" attacks (using whitelisted admin tools like PowerShell)		
Attacks using application vulnerabilities & zero-days (in whitelisted applications)		
Does the product provide additional functionality, such as:		
Identification of grayware (aka dual-purpose tools, toolbars, etc.)		
Root cause analysis		
Attack chain visualization		
OS hardening		
Response functionality (e.g. endpoint quarantine)		
Other functionality		

Question	Vendor A	Vendor B
Deployment and management:		
Can the product be fully deployed on-prem? (if needed)		
Can the product be leveraged from the cloud?		
Does the product support both workstations and servers?		
Does the product come with a pre-populated whitelist (at no additional charge)?		
Will the deployment of the product require cultural changes within the organization?		
Will the deployment of the product require changes in how users request applications?		
Will the deployment of the product require changes in how applications are patched or upgraded at the organization?		
Will the deployment of the tool require the creation of the "gold image"?		
Will the product have to be in the monitor (aka audit) only mode of extended period of time (or forever)?		
How many FTE's are required to manage the solution (per 10,000 endpoints)?		
How many false positives, on average, does the solution generate per day (per 10,000 endpoints)?		
What does it take to create an exception for a confirmed false positive (e.g. time, number of clicks)?		

NYOTRON
SECURING THE WORLD

2880 Lakeside Drive Suite 237
Santa Clara, CA 95054
+1 (408) 780-0750
www.nyotron.com