THREATLOCKER

Allowlisting Buyers Checklist

Application Allowlisting denies all applications from running except those that are explicitly allowed. This means all untrusted software, including but not limited to, ransomware and other malware will be denied by default. Finding an Allowlisting solution that fits your business needs can be challenging. It can also be tough finding a solution that doesn't disturb or interfere with users and doesn't hinder operations. To help you find an Allowlisting solution that does exactly as it says, and works to block cyber threats, we have put together this short checklist.

Below you will find the non-negotiable features an Allowlisting solution should have to help you stay on top of new and emerging threats.

1 Deny by Default

An Allowlisting solution should block any unknown files from executing at the kernel level. For instance, if a threat actor were to exploit a vulnerability such as EternalBlue or get access to your RMM, that software would need to be blocked at the kernel level, not just at the user level. If the solution is only blocking at the user level, it's not a security tool, it's a user behavior tool.

2 Allow by Hash, Not File Name

Rather than allowing files to execute based on the file name, use an Allowlisting solution that automatically blocks files based on unknown hashes. However, there may be instances that you want or need to allow files based on the file name. In this circumstance, make sure you combine it with either a certificate or a process to make it harder for threat actors to replicate.

3 Ability to Block DLLs, Scripts, Jar Files, And Other Types of Executables

An Allowlisting solution needs to be able to block all unknown files to be successful in protecting against known and unknown malware. By blocking DLLs, scripts, etc. by default, we can increase cybersecurity by only allowing what is needed to run.

4 Automatically Track Application Updates

Managing application updates with Allowlisting has previously been viewed as a management burden, taking up significant time. Ensure that you are working with a solution that checks for updates, catalogs them, and allows the updates to run across your network of devices without being blocked. The solution should allow automatic data feeds from users and verify the source of all updates immediately after release.

5 Easy Approval Process

Rather than allowing files to execute based on the file name, use an Allowlisting solution that automatically blocks files based on unknown hashes. However, there may be instances that you want or need to allow files based on the file name. In this circumstance, make sure you combine it with either a certificate or a process to make it harder for threat actors to replicate.

6 Ability to Run Software in a VDI Before Approval With a Risk Analysis

It can be hard for IT administrators to keep up to date with the programs/software users request. Opening the software in a VDI will help administrators quickly understand what the software is trying to access, if it's going out to the internet, it will enable them to check it against VirusTotal, and then either approve or deny it. A VDI provides administrators with the ability to safely test new software and make an informed decision as to whether it should be able to run.

7 Learning Mode

Allowlisting has historically been hard to deploy as creating the allowlist can be time consuming. It's important to ensure you are using a solution that can automatically catalog any existing files across your devices and create policies from the information collected. During the learning process, the administrator can choose to accept the created policies, or fine-tune them. Learning Mode significantly reduces the time it takes to implement an Allowlisting solution.

8 Provide Real-Time Audit

A real-time audit gives IT administrators micro insights into what files are executing across their devices and what files are trying to run. IT administrators can choose to allow or continue denying specific files based on the user's needs. An audit helps IT administrators have a clear understanding of what is running across their users' devices. Ideally, this would be centrally managed from one location in the cloud.

9 24/7/365 Support

ThreatLocker Cyber Heroes are U.S. based and answer your chat or Zoom requests within 60 seconds. They will walk you through any custom configuration, without you needing to read through lengthy administrator manuals or KBs.

10 Managed Approvals

ThreatLocker offers the ability to send approval requests to our Cyber Heroes, 24/7/365. We pick up requests within minutes, run them in our environment, view any risks, and then approve or deny based on your requirements.

11 Simplified and Supported Onboarding

Utilizing a dedicated Solutions Engineer (SE) to help deploy any solution is vital. It is essential that they assist you throughout the entire deployment process and have regular check-ins with you beyond implementation. Our highly trained SE team are well versed in up-and-coming cyber threats. They are dedicated to helping you deploy the ThreatLocker solution with ease and ensure you always have the tools and resources necessary to help you better protect the devices you manage.

12 Combine it With Ringfencing

Allowlisting is incredibly powerful, but it will not stop Windows tools or vulnerabilities from being exploited to misuse applications. Allowlisting solutions should be combined with other security solutions, which will help strengthen and protect your business from the inside out.

THREATLOCKER

To learn more about ThreatLocker's Application Allowlisting and how it can enhance your current cybersecurity stack, reach out to a Cyber Hero today.