WHITE PAPER

In-Depth Analysis of Application Whitelisting

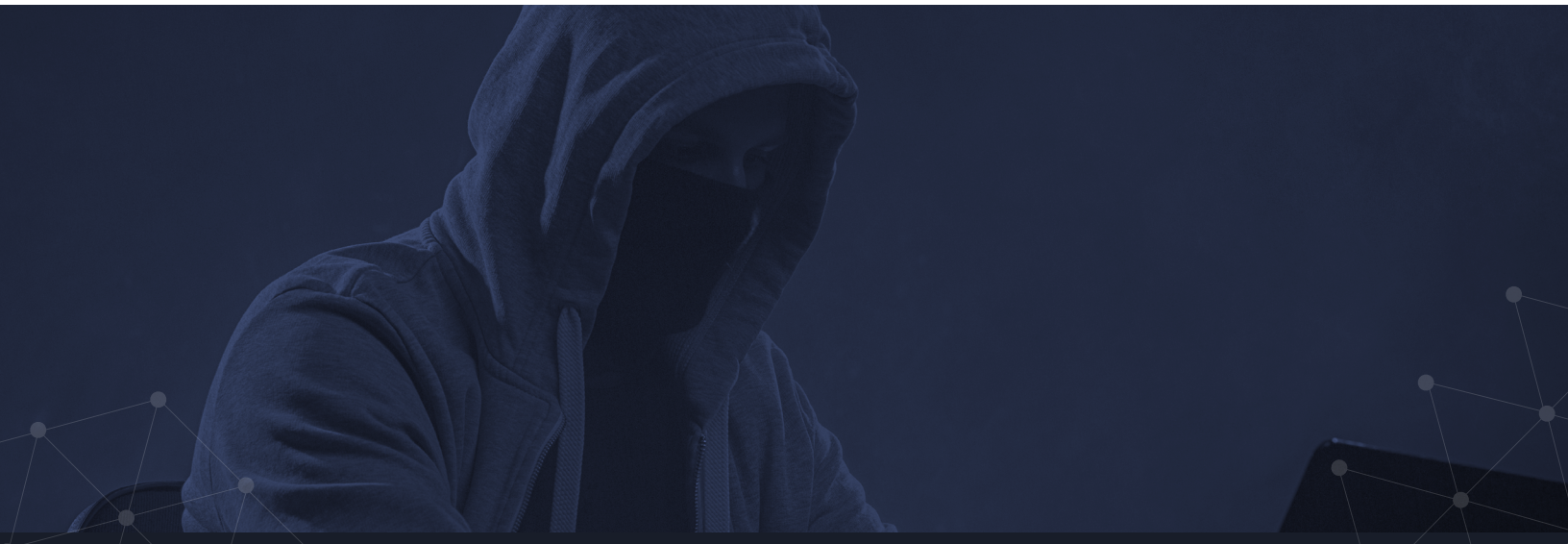
PC Matic FEDERAL

Table of Contents

Introduction

Application Whitelisting is an endpoint security approach that is, for comparison's sake, as old as any other endpoint security approach discussed today. Standing in stark contrast to its sibling approach, blacklisting, Application Whitelisting focuses on a simple task: track good applications and only allow them to execute in an environment. While both approaches are used to secure an environment, both have their potential to benefit the network and negatively impact it depending on the solution and method of implementation. Since both approaches were introduced, the adopted favorite or standard for the industry has been blacklisting several times over. While early on, this decision made obvious sense due to the lack of malware and viruses to track, in today's cybersecurity landscape tracking millions and millions of new malware threats every single day has become a daunting and impossible task. It is time to shift the focus to tracking known good applications and adopt a new but familiar friend into the security family: Application Whitelisting. To begin exploring the reason for this, this whitepaper will break down what Application Whitelisting is at the core, and how it can be successfully implemented and managed to offer more proactive security than a blacklist based security approach while not having a severe negative impact on the network.

95% of organizations will consider deploying an application whitelisting solution



Technical Overview of Application Whitelisting

Application Whitelisting can be broken down into several different components when exploring it on a technical level. While not all flavors of Application Whitelisting are the same, they all take the same basic approach; create a list of known good items, and when something new comes along, compare it to that known good list before allowing it to execute, advance, etc. In today's world, the vast majority of malware, ransomware, etc. is targeted and highly customized for the victim each cybercriminal is looking to attack. Application Whitelisting swiftly prevents these attacks even though they have never been seen before. Depending on the solution, Application Whitelisting can analyze several different attributes to determine what is known good or what is used to make up your known good list.

File & Folder Path Attributes – These attributes are often not the most secure approach to Application Whitelisting, however, they can increase the convenience of implementing this approach. This category encompasses attributes such as File Size, File Name, and File or Folder Directory. An advantage of the use of these attributes is that they provide a bulk method of allowing a known good space or framework. For instance, an entire folder could be set as a known good area that can either allow everything in that folder at the time of whitelisting to execute moving forward or always allow items executing out of that folder depending on the solution. This provides advanced users like software developers with a convenient space to run custom applications, however, it very obviously opens a potential attack point on the machine. Rogue users or cybercriminals could leverage that safe space to run malicious code.

Digital Signature Attributes – These attributes are a much more secure method of easing the burden of Application Whitelisting. Digital Signatures allow software publishers to verify who the software was created by. They also provide additional insight into the state of the executable as any changes to the code cause the signature to become corrupted or no longer valid. The combination of these factors means that creating a trusted list of Digital Signature certificates can give IT administrators the ability to bulk allow known-good software from a specific publisher thus lowering their burden of having to whitelist thousands of individual applications. This can be especially helpful for companies that are creating their own applications for internal use or for sale as a software development company. Digitally Signing code is an affordable practice that doesn't add hassle to the development process. This can, however, drastically increase the security of not only that software but the environment that is employing Application Whitelisting.

Cryptographic Hash Attributes – These attributes include several different options of cryptographic hashes. MD5, SHA-1, or SHA-256, each getting more complex and secure than the former. These hashes serve as a unique identifier for a file and, when a digital signature is not available to use, would be the most secure method of whitelisting applications for an environment. Similar to the digital signature, when any piece of the code is changed, the hash is regenerated and would appear as a brand new file again. This provides incredible security as the one version of the file that has been verified as clean and allowed cannot

be altered and then run within the network. This would be blocked as an unknown hash and require action from an Administrator. It's important to keep in mind the reason that digital signatures are so important is that any updates or changes to these applications that are whitelisted by hash, even when for good reasons, will require a new item being added to the whitelist. This can become cumbersome, but when used in tandem with digital signatures, is a very secure and maintainable approach.

As laid out by the National Institute of Standards and Technology (NIST), a division of the US Department of Commerce, as referenced in SP 800-167 and SP 800-171, a combination of using digital signature attributes and cryptographic hashes provides the most secure and manageable rollout. Using the less specific file attributes can lead to more convenience, but less security overall.

With attributes chosen, now the Application Whitelisting solution goes into action leveraging the combination of digital signatures and cryptographic hashes. Depending on the solution, different technologies may be leveraged to accomplish the execution check, however, in the end, the goal is that when any file attempts to execute on the device it is checked and verified against the whitelist of known good attributes and then if good, allowed to complete the execution. In stark contrast to many blacklisting solutions that will allow unknown applications to execute and then monitor for nefarious behavior or suspicious activity and then alert IT to kill that process and initiate a rollback to undo changes, application whitelisting focuses on preventing any nefarious behavior by blocking the unknown application from executing.

Mitigating False Positives

With Application Whitelisting, the most famous and obvious critique is false positives. A false positive is when something is stopped or not allowed even though it is actually a good application that the user is attempting to utilize with good intentions. With traditional Application Whitelisting solutions, this can become a more arduous task to initially create a robust whitelist and maintain it over time. However, some solutions maintain global whitelists to remove a majority of the work that comes with a whitelisting based approach. With this next-gen style of whitelisting, Admins must only focus on adding very unique or custom applications to their own whitelist and do not need to focus on commonly known good applications. This can provide less headache to the user, and less overall work for IT, which in turn allows for a smoother deployment of a more robust security approach.

However, even with traditional whitelisting solutions, it's important to weigh the pros and cons of mitigating false positives. While it can require work from IT to add in applications on a frequent basis, the alternative is a blacklist based solution that can so often miss malware, ransomware, and other threats and then require IT to not only kill that activity but attempt to recover from changes it made. In today's world of ransomware threats evolving so fast and using complex encryption algorithms, it can be a nearly impossible task to recover from a ransomware attack let loose in the environment without properly maintained backups that are readily available. Meaning, organizations must weigh the potential amount of work and time invested to recover from such threats against IT having a stress free request to allow an additional good application. This comes only with a time requirement from the user who is attempting to accomplish a task they need, and not with the time and stress of a network that needs to be recovered or audited for data exfiltration after a missed threat.

A Layered Approach

In today's cyber landscape, it's important to move on from past notions of endpoint security where one solution or layer was sufficient. Today's cyber threats are adaptive, dynamic, and persistent to obtain their final goal of the attack. Implementing a zero-trust model with your security stack is critical to ensure your environment is not reliant on reacting to new threats as they develop in the wild. Application whitelisting can serve as an outstanding additional layer alongside your zero-trust architecture to incorporate and endpoint security solution that prevents unknown threats in your environment. According to data gathered by PC Matic, 82% of organizations deploy a layered cybersecurity approach to protect their digital assets. This layered approach often contains Firewall, Content-Filtering, Endpoint Security, Backups, and now - Application Whitelisting. With so many reactive layers, a layer focused on prevention can immediately decrease the amount of cyber risk that an organization has.

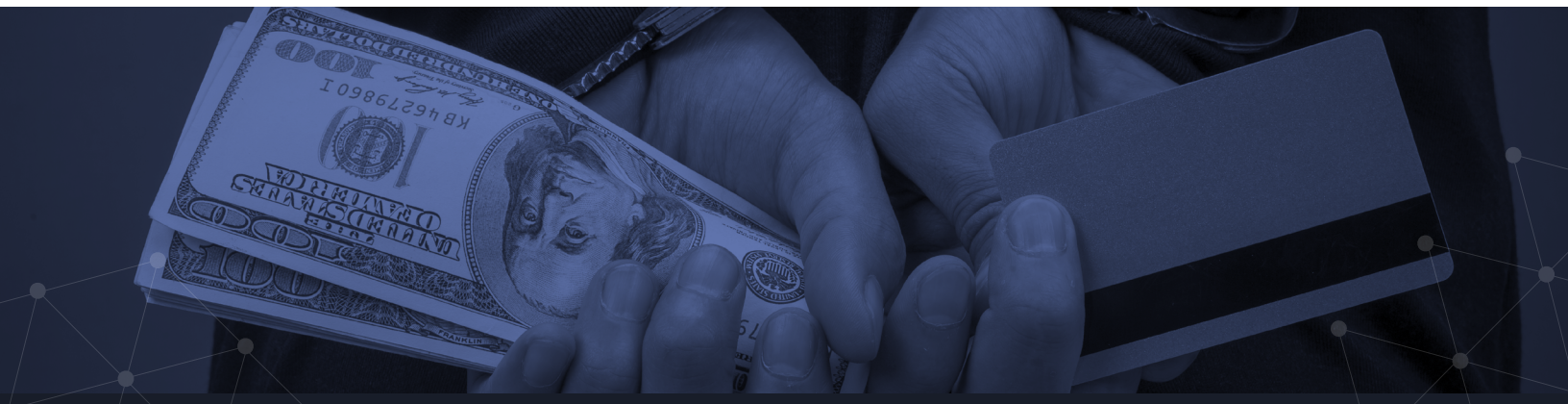
82% of organizations deploy a layered cybersecurity approach to protect their digital assets

Cybersecurity Maturity Model Certification

The DOD is adopting the Cybersecurity Maturity Model Certification (CMMC) framework and PC Matic helps companies achieve levels four and five by meeting criteria CM.4.073 Employ application whitelisting and an application vetting process and CM.5.074 Verify the integrity and correctness of security critical or essential software.

Conclusion

In today's cybersecurity landscape, the traditional blacklist based approach that was successful in the early days of computing is no longer enough to keep digital assets secure. Application Whitelisting provides a more robust approach to securing not only our most critical infrastructures but also some of the most vulnerable targets that may not have a large budget to devote to multiple security solutions or expansive teams. Leveraging the right Application Whitelisting solution can provide any IT team, regardless of budget or size, with the ability to implement this highly recommended approach and focus on preventing malware instead of reacting to threats and recovering. It's important to seek out a newer, next-gen whitelisting solution that can provide this ability, and not require IT Administrators to take on a large burden to manage and deploy. Many solutions are available and all have strengths and weaknesses and different methods to lower the burden; find what is right for you. Shift the focus and prevent, don't react.



About PC Matic

PC Matic's products provide our customers with essential security that enhances the zero-trust model and fills potential gaps left by other traditional endpoint security software. With a foundation in application whitelisting, PC Matic uses a default-deny approach that prevents all known bad and unknown applications from executing. Our patent-pending globally automated whitelist provides a backbone of millions of known good applications to remove the headaches that come with traditional application whitelisting solutions by drastically reducing false positives during and after implementation. This NIST recommended approach combined with a globally automated whitelisted lowers the burden on IT and lowers the barrier to entry for most companies to meet CMMC requirements and build upon a zero-trust mindset by including proactive default-deny protection in their endpoint security stack.