WHITELISTS FOR CYBER SECURITY: THE BAD AND THE UGLY

A 2018 study by Ponemon Institute revealed file-less attacks are on the rise. It states that 64% of successful attacks will be file-based while 38% will be file-less. Equally concerning is the issue raised by the same study which claims that the mainstream cyber defenses currently in place are not adequately effective against in-memory exploits and file-less attacks. Whitelists are currently amongst the most popular defenses used in the cyber security market. This uptrend in utilization of whitelists and similar application control mechanisms is driven by the proliferation of Shadow IT threats, which according to Gartner, will be the root cause of over 30% of successful cyber-attacks by 2020.

Whitelists protect the corporate infrastructure by allowing only approved machines, hashes/files or applications in a predefined list to execute or access data and network resources. Despite the numerous claims of all-inclusive in-depth security provided by whitelists however, one cannot but notice that dependency on the list of approved applications or hashes to enforce protection shares similarities in traits, approaches and shortcomings present in signature-based defenses. These attributes may actually become a security weakness and should not be taken lightly.

Application Whitelists

Application Whitelists are one of the latest additions to the Application Control defense arsenal. Protection works by allowing only files in a pre-approved list of hashes (file integrity checks) and applications (authorized apps) to execute. Applications and files not in the approved list or not matching the approved hashes will be blocked or restricted from executing. However, while such an approach has its merits, numerous vulnerabilities exist that considerably limit the security effectiveness of application whitelists.

One method that attackers often use to elude some less sophisticated application whitelist mechanisms is by disguising malicious apps as one of the whitelisted applications, mimicking the same file name, size, and directory paths. Some more advanced application whitelists may overcome this limitation by using cryptographic hashing techniques and comparing application hashes with the ones in the approved list. Nonetheless, this also has its own shortcomings:

- While arduous, one cannot exclude the possibility that attackers could engineer a malicious application with the same hashes as a legitimate app, thereby tricking the whitelist defenses and slipping past undetected.
- Whenever there is a product update, service pack or patch, the hash of legitimate applications will change, resulting into false positives and alarms generating unnecessary commotion.
- Cryptographic hashing techniques have high overhead and are considered ineffective when it comes to protecting applications in memory.

Additional operational overheads

The effectiveness of application whitelists is highly dependent on the approved list. Consequently, additional maintenance efforts are needed by the IT team regularly (even hourly or daily in some instances) to keep:

- The hash-list updated every time legitimate products including the OS are upgraded, updated or patched.
- The application list updated to:
  - Remove applications not used anymore; otherwise, they can still be used and exploited.
  - Include any new applications that are onboarded, even if these will be used temporarily by contractors, for example, that will be connected to the organization’s network; otherwise, working operations might be blocked or unwarranted false positives and alerts may be generated.

Exploits via legitimate binaries, apps and files

Research by eSentire revealed that 91 percent of endpoint incidents detected in Q1 2018 involved known, legitimate binaries. In fact, malicious users may exploit trusted tools, which are in the approved whitelist, to run their attacks:

- Legitimate applications, including tools built into MS Windows OS like PowerShell, serve to automate administration tasks and often cannot be blocked without hindering company operations; leading IT teams to whitelist them. In some cases, such tools may also end-up automatically whitelisted since they are part of an already trusted application; so if they are exploited, whitelists are incapable of blocking them.

- Attackers may leverage PowerShell to cloak their activity and build malicious scripts to deliver their payload, evading whitelists and signature-based defenses by running in-memory exploits and obfuscating command-line parameters to run file-less attacks.
- Application whitelists cannot restrict memory access from attackers and offer little-to-no effective protection against attacks that:
  - Read data being worked on by legitimate applications directly from memory (RAM scraping)
  - Scrape data from the swap file, leveraging commonly accessible tools like Mimikatz.

IP/Protocol Whitelists

Whitelists alone are often limited in protection against attacks coming from legitimate machines, ports and protocols. Some malware like EternalBlue can exploit vulnerabilities in legitimate windows protocols (e.g. Server Message Block (SMB) protocol) and have been used as a channel to direct numerous attacks; including WannaCry, UIWIX, Petya/Not Petya, Emoter and Trickbot in 2017/2018.

Exploits via legitimate machines and endpoints

IP whitelists are another variant of whitelist-based cyber defenses. In principle, their operational approach is similar to that of application whitelists; but enforcement is via whitelists containing approved IPs, Subnets, Mac addresses and sometimes URLs.

IP whitelists are mostly used to secure against rogue devices or limit and control access on a machine-by-machine basis, restricting to specific network areas and operations. However, IP whitelists also have numerous limitations in addition to those of other whitelists mentioned earlier:

- **Operational restrictions:** Policies based on an IP Whitelists may restrict the use of DHCP for IP allocations in an organization.
- **False positives:** A DHCP setup may invalidate the protection if the list of approved IPs is not dynamic or based on ranges. This may also generate false positives or unwarranted blocking of legitimate endpoints.
- **Operational overheads:** Initial setup requires the definition of every single legitimate endpoint and endpoint group. This may call for additional effort to keep the whitelist updated and may become unmanageable with a DHCP setup.
- **Misallocating IPs:** The dynamic allocation of IPs may also limit access to legitimate users while allowing access to unauthorized ones should a refresh of IPs occur, preventing the whitelist policies from being updated accordingly.
- **Outdated, legacy setups:** The IP whitelist is like a hardcoded policy and control will continue to be applied according to the approved list. Legacy setups may become a

vulnerability if not reviewed and revisited frequently. Such legacy setups may be the result of:

  - New machines added or decommissioned
  - New people onboarded or leaving
  - Contractors and temporary workers

  All the above are examples where new devices are hooked to the company networks while others are not in use anymore, which may lead to protection vulnerabilities. For example, contractors and temp workers may retain network access after leaving if their IP and access rights aren't managed or set to expire.

- IP whitelists alone are not able to stop attacks and exploits coming from legitimate endpoints:
  - The privileged access that endpoint users and insiders have for the execution of their everyday tasks makes a network more vulnerable to attacks coming from its endpoints.
  - Since IP whitelist protection is based on an approved list of authorized machines and IPs, whitelist defenses will not detect an attack originating from a legitimate/authorized machine as a threat and thus will not block the exploit.
  - Attackers gaining access to legitimate machines may use OS built-in kits like PowerShell to retrieve and execute malicious code, even from remote sources. Since attacks manifest as in-memory exploits, these are often file-less and, therefore, have no physical storage footprint and generate no physical file. Consequently, any protection policies and restrictions operating on criteria like IP and/or application whitelists, physical disk-space, file names or file-size will not be effective.

Limited forensic data and telemetry

One final thought is on the limited telemetry that whitelists seem to provide for forensic analysis. Forensic analysis is a very important process in the setup of thorough protection and future countermeasures. Amongst key contributions, forensic data is crucial in the definition of approved lists for whitelists. The downside is that whitelists provide no live-detection forensics and limited postmortem analysis for investigators, as opposed to other cyber security solutions. Once past the filtering, whitelists provide no telemetry on activity at run time and what was potentially compromised by an attack.

The way forward…

Conventional whitelist protection is not comprehensive enough to offer wide-scale protection and peace of mind.

The inability to detect and block foreign or malicious code executing at run-time is a considerable shortcoming in today's cyber security landscape. The dependency on an approved list of trusted IPs and applications, both of which can be spoofed and legitimate systems exploited, is a serious risk to consider.

Whitelists can easily become time-consuming to maintain with a large dependency on the IT team to keep it up to date, resulting in added management overhead and false positives as the organization scales up.

For effective protection, organizations need cyber defenses that are not dependent on a manned list. Such mechanisms must:

- Provide deterministic and preventive cyber security that is effective in the time of need.
- Provide in-memory protection against malicious attacks including file-less, RAM scraping and more.
- Monitor activity at run-time for wide-scale effective protection on demand.
- Fully capture forensic artifacts in context at point of attack for detailed telemetry and deep-dive insights.
- Be understood and thus trusted to be effective from day-one of deployment.
- Be measurably comprehensive in security coverage and long-term protection.
- Be able to notify users (local, regional, functional, corporate teams) about the real (immediate) priorities consistent with operational capacity; i.e., without inundating them with false alerts.
- Be scalable yet low in resource consumption.
- Provide protection directly at the endpoints with a lightweight kernel Sensor.

Introducing Digital Immunity

"Digital Immunity Protect" is a deterministic, preventive cyber security endpoint protection solution that verifies the integrity of trusted code executing in memory at runtime using a lightweight Sensor running in the kernel. Digital Immunity Protect prevents advanced threats including Advanced Persistent (and Volatile) Threats (APT/AVTs) and zero-day attacks from executing before the damage is done and hardens you operating systems and related applications when most vulnerable: in memory at runtime on your endpoints.

By applying patented Digital DNA Mapping and in memory protection of all executable code, Digital Immunity Protect automatically creates Digital DNA maps enumerating all the core foundational components of operating systems and related applications – creating an alternate digital representation of all trusted executable code. These Digital DNA maps are provisioned to endpoints and compared to the actual code in memory, immediately prior to execution, during execution and on its exit from memory. Any code that mutates at runtime when compared to its original DNA Map is blocked (depending on policy) from executing – preventing virtually all foreign or malicious code, even zero-day and novel strains of malware, from executing and exploiting vulnerabilities in your operating systems and related applications. An alert will be generated and can be viewed in the DI Control Center (Console) or in your existing SIEM.

This allows for in-memory run-time protection and detailed in-context forensics far superior to those of conventional whitelists, allowing Digital Immunity Protect to prevent threats other traditional solutions cannot.

Unlike conventional endpoint protection typically deployed in organizations, Digital Immunity Protect does not need lengthy A.I. malware learning processes, manual whitelist definitions, signature downloads or behavioral analytics. As a result, it uses a fraction of the system resources and time to setup versus conventional whitelists and A.I. defense mechanisms – making it fully effective from day one of deployment.

Digital Immunity Protect is highly scalable and can be deployed on premise or in the cloud to effectively protect both SME and Enterprise infrastructures with low maintenance overheads, unlike whitelists and other counterparts.

Some key aspects of Digital Immunity

- **Prevent and Detect** the Execution of Foreign or Malicious code including Ransomware, File-based or Fileless
- **Effective immediately on day 1 of deployment –** no dependency on historic malware-data analysis, no lengthy A.I. learning process needed.
- **Active in Memory Protection at Runtime –** when applications are most vulnerable
- **No Pre-existing knowledge** of exploits or vulnerabilities needed to prevent cyber-attacks against your OS and applications
- **No Dependency on signatures or whitelist databases**
- **Threat Intelligence directly at your endpoints –** Full capture of forensic artifacts at point of attack irrelevant of IP, file or application running
- **Deterministically remediate** at the Endpoint, i.e. right at the source of exploit
- **Lightweight on system resources -** Sensor runs at kernel level with no resource-demanding historic data analysis needed
- **Intelligent alert management -** Notifies you of the real immediate priorities; does not inundate you with false, superfluous or repeated alerts

Sound too good to be true? Don't just take our word for it – we invite you to try our solution! Request a Digital Immunity demo now.

Have a query? Send us an email at Info@digitalimmunity.com
Want more info? Check our Datasheet or visit our website: www.digitalimmunity.com