PC Matic PRO

WHITELISTING

Whitelist Protection

The foundation of the antivirus industry has been blacklist based protection since the early stages of security software. This approach is still heavily relied on today even with the flaws it contains. Endpoint security and antivirus protection must evolve to address today's threats PC Matic Pro employs a whitelist providing default-deny protection to stop all unknown malware before execution.

Blacklist vs. Whitelisting

Blacklist's Critical Flaw

The critical hole in the blacklist architecture is how it deals with unknown applications. A polymorphic virus infects a computer and changes/morphs its signature to evade blacklist detections.

Ransomware continues to evolve with new variants that have not yet been detected by a blacklist. Cyber criminals often use new samples or strains of ransomware for high value targets.

Using unknown malware against traditional approaches increases the likelihood drastically that the attack will have success.

The blacklist can't keep up with the amount of unknown threats that appear on a daily basis.

How Whitelisting Works

When a process starts to run, PC Matic Pro first checks a signature whitelist, basically a list of companies that write trustworthy software.

Next, it checks a whitelist of unsigned applications. If the application is not on either list, it is blocked from execution, and a message pops on the endpoint.

The sample is uploaded to our USA based malware research team to categorize within 24 hours. End users and IT employees can locally whitelist the sample for faster turnaround times.

PC Matic Pro has proven the whitelists' efficacy through perfect scores on the AV Comparatives and Virus Bulletin tests.

pcmatic.com/pro

info@pcmatic.com

PC Matic PRO

2018's Awards

Market Leader for Anti-Malware Software

Most Innovated Security Software Product

Threat Detection 2018

AV-Test Certification Windows 7 Home

What about False Positives?

The normal knock against whitelisting solutions is on False Positives and management needed for the whitelist. PC Matic's Globally Automated Whitelist aims to take on the majority of the work by staying updated with good software our Malware Research team sees. In practice, unique or proprietary software may need to be locally whitelisted by the IT Admin before deployment, but our Good File Accuracy (correctly allowing good applications) has tested very well with third parties.

Virus Bulletin	AV Test
99.744%	99.996%

Time to Mitigation

An important question to ask when weighing the negatives of a whitelist based solution and dealing with false positives is how long does mitigation take. Our stance has always firmly been that dealing with a False Positive is better than a False Negative.

False Positive	False Negative
11 Mouse Clicks 15 Minutes Manually 24 Hours Automatically	Countless Overtime Hours Weeks of Data Recovery Drastic Financial Costs

Application Whitelisting - The Best Practice

- US-CERT - Encouraged government agencies, as well as businesses to implement application whitelisting technology to avoid falling victim to similar attacks (US Power Grid Attack).
- NSA - "Application Whitelisting offers tremendous security value: Blocks most current malware, Prevents the use of unauthorized applications, [and] Does not require daily definition updates…"
- Homeland Security - "Application whitelisting – Whitelisting is one of the best security strategies because it allows only specified programs to run while blocking all others, including malicious software."
- New Zealand CERT - Dynamic whitelisting employing trusted ownership can help you prevent unauthorised code execution without making IT manage extensive lists manually.