Protecting the LAW

PC Matic PRO

Customer Success Stories

Iberville Parish Sheriff's Office

"We've been using PC Matic for 3 years. We were using Norton at one time, we were using Kaspersky and we were getting malware and adware on a regular basis. When we started using PC Matic, the ransomware was never an issue, malware was never an issue. We could really see the difference. We didn't have one issue with PC Matic trying to block a particular program. The whitelist works perfectly. The security and performance is definitely above and beyond what I've seen in other products before."

- Tommy Favaron
Director of IT Iberville Parish Sheriff's Office

Cyber criminals have begun to specifically target those who protect us, our police departments. Local law enforcement computer systems often contain a large amount of deeply private information ranging from violent crime reports, 911 call logs, ongoing investigation reports, and access to nation information databases.

Ransomware attacks on police departments typically don't result in compromised information or evidence, but experts believe it is only a matter of time before cyber criminals start stealing this information as well as holding it for ransom.

Cyber Criminals Targeting The Police

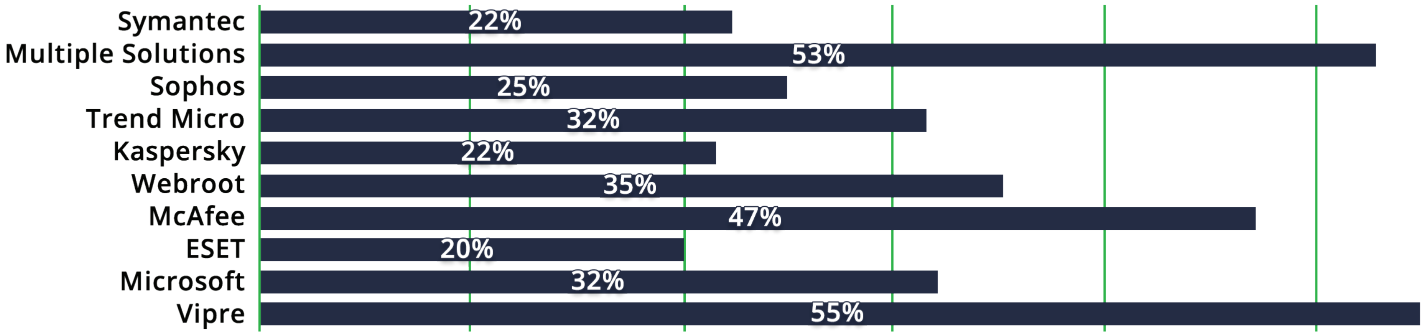
- ✓ According to cyber security experts, new variants of ransomware like MarsJoke have been introduced to specifically target state and local government agencies in their infection campaigns.
- ✓ Police Departments are especially lucrative for cyber criminals when targeting state and local government according to Alexander Volynkin a senior research scientist at Carnegie Mellon. Because departments often need to act quickly with their data it can create a sense of urgency to recover it and thus pay the ransom.
- ✓ Ransomware is expanding at a blistering pace according to statistics from the US Government. 2016 saw more than a 300% increase in attacks compared to 2015; and this year is set to continue the trend.

pcmatic.com/pro
info@pcmatic.com
855-865-6655

Legacy Antivirus Has Failed

The amount of ransomware variants that are being introduced into the world on a daily basis is staggering, and it's not surprising that the traditional blacklist approach can't keep up. In a recent survey by KnowBe4 you can see the percentage of organizations experiencing a ransomware attack by current AV solution.

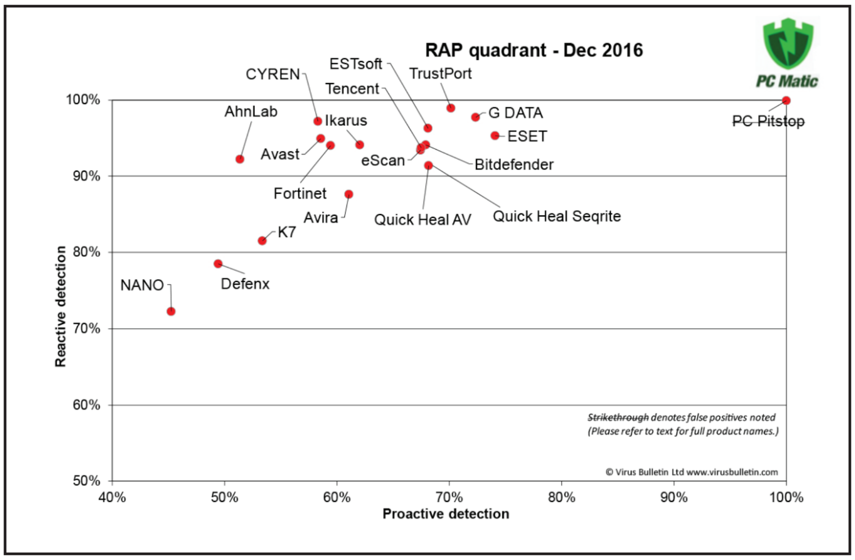
Percentage of organizations experiencing a ransomware attack (by AV solution)



*KnowBe4 Survey of 500 Organizations May 2017

A New Approach is Desperately Needed.

With PC Matic Pro we are providing default-deny application whitelisting on a global level, which removes the overhead needed to implement a whitelisting solution and maintain it over time. We stop all unknown software from executing on the endpoint and only allow known good applications that are on our whitelist.



You don't have to take our word for it; independent testing houses are testing security products frequently to see how effective they actually are. If products you're considering aren't routinely tested it's important to ask why. We offer up one recent test of our product here from Virus Bulletin to begin your deep dive into detection rates.

Ransomware Tampering with Evidence:

Cockrell Hill Police Department

The Cockrell Hill PD serves a town of roughly 4,300 people outside of Dallas, Texas. In January of 2017 one of the department's servers was hit with a variant of the OSIRIS ransomware. Hackers were demanding a ransom of $4,000 to provide a decryption key and unlock the files. After consulting with the FBI and the IT staff, the department decided to wipe the server and not pay the ransom, deleting 8 years of photo, video, and document evidence.