Securing the Healthcare Industry

PC Matic PRO

Ransomware Attacks

Erie County Medical Center – Buffalo, NY

Although Erie County Medical Center (ECMC) didn't pay the $30,000 ransom demand, the intrusion that brought down the hospital's computer systems came with a major expense. ECMC officials have estimated the expenses tied to the incident were nearly $10 million.

Presbyterian Medical Center – Los Angeles, CA

As probably one of the most well-known victims of a ransomware attack, Hollywood Presbyterian Medical Center was one of the first publicized victims of ransomware. In order to recover their systems, they paid the cyber criminals $17,000.

Caro Community Hospital – Caro, Michigan

Hackers don't discriminate based on a city's population. That was proven when a ransomware attack hit the small community of Caro, Michigan. After locking the three medical facilities' systems, the cyber criminals made a ransom demand of $120,000. Operations were almost back to normal, two weeks after the attack.

The medical industry has become the most frequently targeted industry for cyber attacks, specifically ransomware. With a large number of users, devices, and reliance on technology, medical facilities are particularly appealing to cyber criminals.

Cyber criminals know that targeting medical facilities means lives can be at risk, which creates a sense of urgency. Hackers feed off of this, knowing many medical centers will pay the ransom, instead of compromising patient care.

Medical Facilities Named No. 1 Target for Cyber Attacks

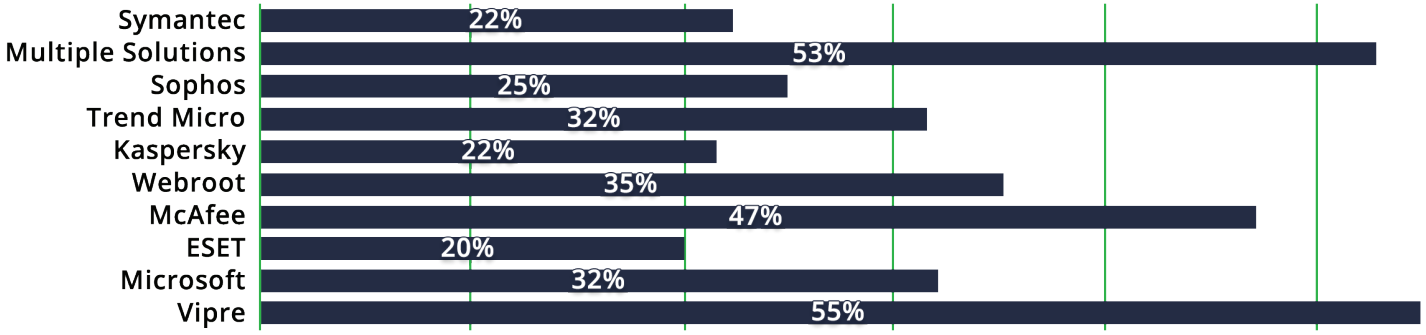
- Malware attacks on the healthcare industry carry potentially catastrophic risks including the compromise of patient data and costly HIPPA violations.
- Malware attacks have become a dual threat for the healthcare industry. Not only is malicious software installed, but there is also the growing risk of patient data being leaked in the process. This has been the latest concern expressed by Pacific Alliance Medical Center, Women's Healthcare Group of Pennsylvania, Plastic Surgery Associates, and Salina Family Healthcare Center – just to name a few. All of these facilities were targeted by malware, and after proper investigation found thousands upon thousands of patient files were left compromised.

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)

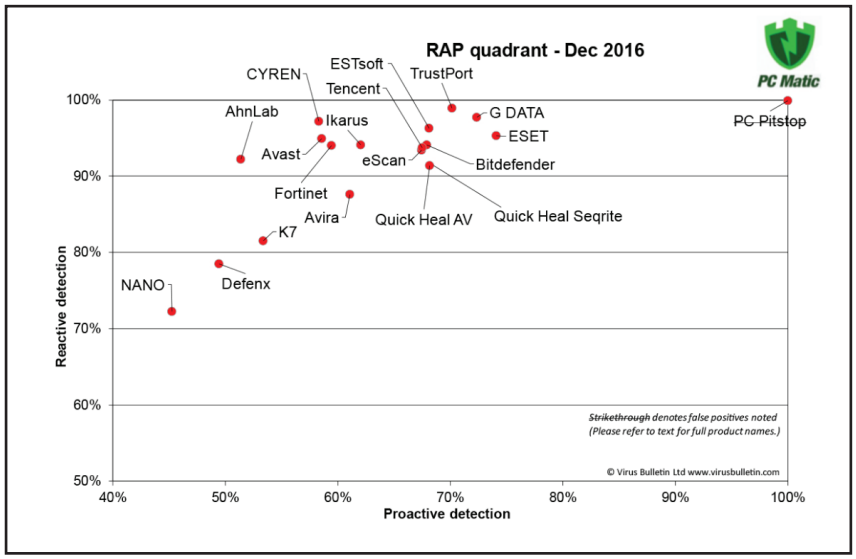


*KnowBe4 Survey of 500 Organizations May 2017

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.



> **"We know the medical environment is being targeted. The blacklist approach is not sustainable, and has become a losing battle. It is time the industry implement a default deny approach, like what can be found with PC Matic Pro. Whitelisting offers a high level of network control, many medical facilities have never seen."**
>
> ***– Dodi Glenn, VP Cyber Security (PC Pitstop)***