

SecureAPlus gets top marks for ransomware, crypto-miner malware, and bashware tests

After a series of cybersecurity tests that cover ransomware, cryptominers, and bashware threats, SecureAPlus is receiving the highest awards for all three rounds of testing

June 26, 2018 - AVLab, a Poland-based cybersecurity testing firm, [has recently released the results](#) of its extensive tests of endpoint security solutions against three significant and prevalent threats in the industry today. The tests involved multiple industry-recognized cybersecurity vendors and tested them against ransomware, cryptominers, and bashware malware tests.

The SecureAPlus application control and cloud anti-virus are among those that have scored the highest awards from all three tests.

In conducting its tests, [AVLab and its newly introduced testing platform, Check Lab](#), have created scenarios that reproduce the real behaviour of both malicious software (malware) and a typical user. All file samples used were extensively checked to be malicious, and they classified cybersecurity software detections into early, middle, and low levels to indicate at which point a threat was stopped.

The year 2017 is infamous for the outbreak of a slew of destructive ransomware, such as Wanna Cry, that swept across the globe. The damage is done; both actual money lost as well as productivity lost cost was in the billions.

The threat of ransomware attacks will continue to be prevalent in 2018, and the years to follow, AVLabs tests were designed to test the effectiveness of endpoint security solutions in preventing their host system from being infected unknowingly by these threats. SecureAPlus performed well, being able to detect threats earlier while blocking the majority of the threats before they can run on the system.

The year 2017 also saw the growing trend of cryptominers malware.

In the advent of the increasing interest in cryptocurrency, malicious parties have since used it as an opportunity to use malware to profit from CPU & GPU performance of infected machines.

Attention has only grown in 2018 and shows no signs of slowing down so far. On the tests conducted, SecureAPlus did very well in first level detections while managing to detect the rest of the threats at the low level.

With none of the threats managing to run, SecureAPlus has also secured the highest rating from AVLab's cryptominer malware test.

Last but not the least, with the introduction of the [Windows Subsystem for Linux \(WSL\) feature](#), Microsoft has virtually opened a potential new vector to infect Windows Systems. The benefits of WSL are undoubtedly tremendous, especially for developers. Due to the nature of the attack, SecureAPlus was among the solutions



that were able to detect and prevent it from launching to deliver its payload and earning the highest marks for the bashware test.

[SecureAPlus](#) continues to improve on its core features of application control and to whitelist to bolster further the defences it provides as layers of security to endpoints.

As newer and unknown threats emerge, early detection has become even more difficult for endpoint security vendors.

The type of protection that SecureAPlus provides at the lower level of computing continues to be a reliable last line of defence for Windows users and maybe what enterprise and home users alike may need to have in a cybersecurity climate where threats like malware and ransomware are rapidly produced and iterated.

Press contact Raissa Sutopo - raissa@secureage.com

About SecureAPlus

[SecureAPlus](#) is a free security software developed by SecureAge Technology that protects PCs from malware & viruses with its powerful but easy to use Application Whitelisting and reliable detection rates of more than ten cloud Anti-Virus engines with Universal AV. It leverages the power of the cloud allowing for low resources used and compatibility with other installed anti-virus and anti-malware applications, making it the perfect security upgrade for any Windows PC.

About SecureAge Technology

SecureAge Technology is a rapidly growing data security company that places security and usability on equal footing. Headquartered in Singapore, we are trusted by governments, research institutes, and forward-thinking organizations to protect them from the most advanced and persistent cyber threats in the world. What makes SecureAge different, is we have built a reputation for data-centric and intuitive security solutions that protect data not only when it is stored, but also when it is in use, and in transit. We've achieved this by holding strong reign on our belief that users shouldn't have to become cybersecurity experts to escape data liabilities. Instead, encryption should be inherent, invisible, and instinctive. To protect data when it is most vulnerable, security must take place at the file-level, operate silently in the background, and support the way in which people collaborate. That's why our users can divert their resources to focus on other challenges – SecureAge users enjoy 100% file-level security, every file, every place, and every time. For more information visit www.secureage.com and follow us on [LinkedIn](#) and [Twitter](#).