

SecureAge introduces ‘Recommended Actions’ for endpoint protections to relieve user anxiety for remote or office-based workers

June 6, 2020 - [SecureAge Technology](#), a leading global data and endpoint protection company, has announced a key update to its flagship SecureAPlus Endpoint Protection Platform (EPP), to reduce user anxiety for remote or office-based workers. ‘Recommended Actions’ has been added to its Application Whitelisting to provide additional real-time guidance on how to respond to prompted alerts when a non-trusted file is identified. The new feature is particularly valuable for people working from home, outside the usual oversight of the enterprise because of COVID-19.

“SecureAPlus end point protection is designed to provide end users – wherever they are working - with 100% protection from ransomware, keyloggers and other malware by simply blocking all previously unknown processes,” said Dr. Teow-Hin, SecureAge founder and CEO, “With Recommended Actions we go further to reduce stress for both end users and IT admins by providing intelligence-led guidance based on our analysis of millions of viruses together with collective malware research.”

SecureAPlus combines three core features for complete endpoint protection. An AI trained APEX engine analyses millions of live virus samples collected from customers and research, while a universal anti-virus platform (AV) harnesses multiple leading cloud-based AV engines to detect and block known threats. And finally, advanced interactive Application Whitelisting blocks any threat not detected by the AV or AI engine.

While SecureAPlus already prompts users to ‘block the action’, ‘allow the action once’, or ‘allow the action always’, users may still have concerns about making the wrong choice. So, the new Recommended Actions feature now provides guidance based on SecureAPlus threat intelligence data. For example, the ‘Unblock & Trust’ recommendation is based on clean AV and the AI engine scans, with the option to ‘Get a Second Opinion’. If the file is considered dangerous or suspicious, a ‘Continue Blocking’ recommendation is displayed.

In addition to Recommended Actions, SecureAPlus Version 6.2.0 includes further updates for Enterprise. A new Vulnerability Assessment feature checks programs against common vulnerabilities and exposures (CVEs), while optimisations allow endpoints to securely boot up faster after a Windows Update and improve the treatment and behaviour of Trusted Installers & Trusted Applications. Recommended Actions is available to SecureAPlus Pro, Essentials, and Lite users with Version 6.2.0 and above. Individual users can download SecureAPlus at www.secureaplus.com.

Press contact Raissa Sutopo - raissa@secureage.com

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](#).