They thought it was undetectable. They thought it was unstoppable. But the cybercriminals who ingeniously created Flame to remain under the radar were wrong.

But, it wasn’t the typical perimeter defense systems that stopped the malicious attack. In fact, no known traditional security measures have stopped Flame, except one.

To date, Flame Malware is the largest, most sophisticated cyber weapon to ever be developed. Masquerading as a Microsoft security certificate, flame bypassed 43 of the most trusted antivirus solution for nearly two years.

Flame is the most recent attack consuming IT security professionals, but it’s not the first and certainly not the last. Cybercriminals are become more adept at finding ways around standard security measures. Their attacks are more persistent and targeted and backed by deep pockets and specific agendas.

Information security expert Eugene Kespersky, whose team of researchers discovered Flame, told attendees at a [cyber security conference](http://www.timesofisrael.com/experts-we-lost-the-cyber-war-now-were-in-the-era-of-cyber-terror/) sponsored by the Tel Aviv University’s Yuval Ne’eman Workshop for Science, Technology and Security that the Flame threat is just the beginning of unprecedented cyber-terrorism by smarter and stealthier criminals.

But, there was a single solution that did stop Flame and has consistently and successfully been stopping advanced persistent threats: Application whitelisting .

Why did [application whitelisting](https://www.bit9.com/products/bit9-parity-suite.php) work, when all the others failed? The answer is simple. By using a trust-based, endpoint security, only known and trusted applications are permitted to operate, stopping any unknown sources from permeating the enterprises networks, intellectual property or other targeted data. Traditional antivirus programs rely on blacklisting known malware. Meaning IT professionals must be aware of the existence of the malware in order to create codes to block it. In the case of Flame, it took over two years for IT professionals to detect the malicious activity, leaving thousands of computers and networks vulnerable to its activities.

With trust-based whitelisting technologies attempts by viruses, Trojans, Stuxnet, application exploits, custom attacks, zero-day threats and even Flam are thwarted and target-rich information protected. Besides keeping the enterprise safe, many application whitelisting programs include monitoring software which will keep IT professionals alerted when an attempt has been made.

While APTs are keeping security experts awake at night, those who have instituted application whitelisting technologies to their security protocols are resting easy.