



WHITE PAPER

Does CSA'S End-of-Life Signal The End of HIPS?

27 September 2011

Written by:

Fatih Comlekoglu
Chief Software Architect
Blue Ridge

With software maintenance ending this December 2011, the product known as the Cisco Security Agent (CSA) reaches End of Life. Known as Okena StormWatch and first introduced in late nineties, StormWatch was acquired by Cisco in 2003 and re-named as CSA. Other security vendors acquired similar Host Intrusion Protection Systems (HIPS) products of the same era. CSA's end-of-life is also the confirmation of an end of an era for HIPS even though similar HIPS products are still being marketed by the same security vendors.

The new owners of the acquired HIPS products never improved them to address today's threats. Designed to address the malware for Windows 95 and Windows 2000, these HIPS products stayed frozen in time. As Windows evolved over a decade, with Vista and Windows 7, Microsoft introduced new protection capabilities including DEP (Data Execution Prevention), ASLR (Address Space Load Randomization), preventing arbitrary code execution in exception handling paths, and UAC. After all these changes, HIPS's decade old defenses primarily developed for Windows 95 and Windows 2000 era malware, became irrelevant. As the Windows protections improved, the HIPS concept was helpless and useless in tackling a new generation of malware that no longer needs local administrative rights to cause damage.

HIPS products were too focused on the antiquated application anomalies of the Windows 2000 era and on unpredictable application behaviors. This resulted in per application tuning of rules, false positives, and asking users to make advanced security decisions through pop up dialog boxes. Rules and exceptions needed to be formed per application. When applications were updated, this created a tremendous burden on administrators to manage the thousands of application rules on a day to day basis. The millions of events generated daily paralyzed administrators of even the smallest of deployments. Outdated techniques of HIPS mistakenly concluded that the mostly normal behavior of legitimate applications were malicious and thus interfered with perfectly normal applications. To eliminate HIPS interference with running applications and the resulting false positives, administrators spent countless hours crafting application specific rules and exceptions. As the applications were updated, administrators had to preserve old rules and establish new rules and exceptions to support multiple versions of the same application. The new HIPS rules and exceptions meant more time consuming regression testing to ensure no side effects. But more exceptions meant more donut holes that resulted in security gaps - making the use of HIPS for protection immaterial.

THE MYTH OF WHITELISTING AND THE NEED FOR THE NEXT GENERATION OF WHITELISTING

Today, the same experts that led us to the HIPS Cul-de-sac are now telling audiences that traditional White Listing is the silver bullet for malware defense. Although HIPS and traditional White Listing are vastly different technologies, they both have the same weakness: both have significant administrative overhead for day-to-day operations to a point that the management of the product itself becomes central point as opposed to protecting the enterprise. While HIPS administrators had to worry about constantly tuning HIPS rules, traditional White Listing products require administrators to be concerned about software updates and security patches and ensuring new signatures are available to end points before the patches and updates can be applied.

Traditional White listing solutions rely on a myth that if an application is signed and approved, the application is safe. Today's malware can easily hi-jack perfectly legitimate and signed White Listed applications in run time. The hi-jacked application can encrypt user's data and ask for ransom in the form of an encryption key. A hi-jacked application can "migrate" to another perfectly White Listed application by altering Windows registries, by performing code injection, or by modifying the memory of a running process. Or a White Listed application could peek into the memory of an important financial application to steal financial data or steal content of user's files by reading and uploading to a server on the Internet. Traditional White Listing is completely defenseless against the new generation of malware that embeds itself in Adobe PDF, Adobe Flash, Music or Video files or Microsoft Office Documents. Aside from a false sense of security for users, traditional White Listing has draconian consequences. At first sight, permitting only legitimately signed applications to run may be what the system administrators strive for. But in reality, for productivity reasons, users will need to run additional non-standard applications, download PDFs, Office documents, pictures, and watch training videos. This shift will lower productivity and increase help desk costs while creating an operational quagmire for administrators.

BLUE RIDGE'S APPGUARD IS THE NEXT GENERATION

Award winning AppGuard Enterprise and AppGuard Consumer are next generation endpoint protection solutions designed to give users freedom and flexibility, yet providing the best protection for the endpoints. AppGuard protection relies on dynamic White Listing capabilities combined with patented anti-malware defense techniques that include virtual user space protection, out-of-the box policies for protecting user and system resources, as well as application protection with enhanced memory protection and control. The lowest administration overhead in its class, AppGuard Enterprise includes a central policy management and monitoring system with predefined policies and rich security audit reporting capabilities. In comparison to traditional White Listing or HIPS, AppGuard Enterprise offers unmatched simplicity with set-and-forget management capabilities that enterprises have been seeking for years. As far as malware protection is concerned, it achieves a more stable and secure environment than White Listing without the operational issues.