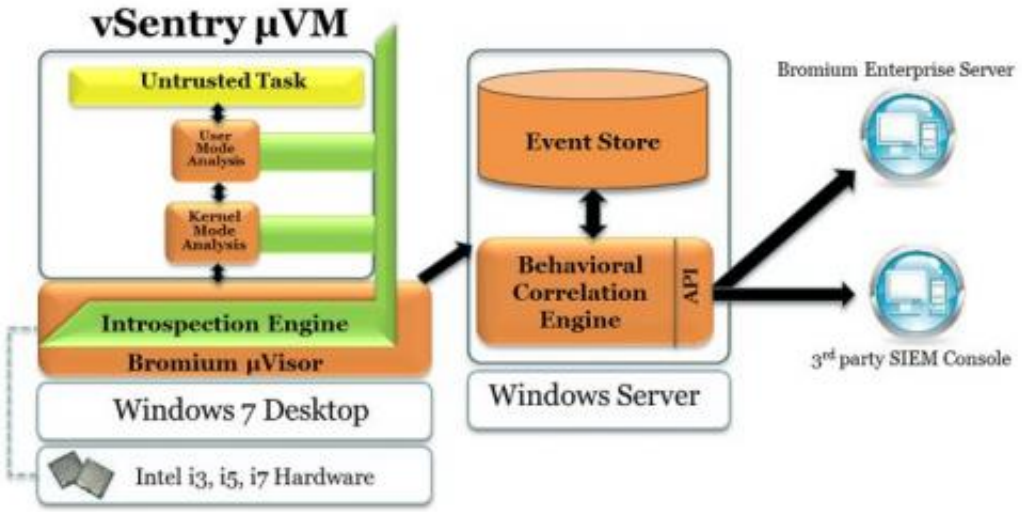
Bromium sets up business net around malware (Update)

September 19 2012, by Nancy Owano



Credit: Bromium

(Phys.org)—Bromium has announced the availability of a product intended to make a significant difference in how enterprises cope with relentless attempts to attack their systems with malware, burdening IT departments and preventing employees from carrying on business as usual. The only headaches inherent in Bromium's product might beset rival security companies that do business in anti-virus software and data protection. Ian Pratt, Bromium co-founder, said, "Traditional security products rely on being able to look at any document in advance and decide whether it contains malicious code which can be identified by `signatures' already reported.... Yes, a bit like after the horse has bolted."

Bromium's software product is called vSentry, and the technology approach rests on a micro-virtual machine—an isolated environment—that protects the underlying operating system and whatever content is stored on the machine from malware.

The microVM isolates attacks, trapping malware and analyzing it so that IT staff can explore it further without interruption to employee computer users. According to its designers, a PC user at a company would not be aware that it is installed. The machine tracks employee use of the web. All the data from a website visit is contained. vSentry places each document into this virtual machine. If someone clicks a bad link, the micro-VM will keep it until the IT administrator views and disposes of it. The virus cannot escape from the safety shield of this environment to enter the actual computer.

The company's target is the enterprise customer, because that is where the opportunity lies for the virtual machine approach. vSentry is licensed per-user, enterprise wide, and priced according to volume. Security teams may have ample expertise but they cannot actively block attacks they never saw before. The vSentry appeal is not just that employees can be free to work without fear of bringing up viruses, but that the information captured for the dashboard provides information on the malware attempts. The company says that the information via vSentry's "Live Attack Visualization and Analysis" (LAVA) feature delivers information about the attack's origin, techniques, and targets.

Rather than reducing the need for a security team, the product gives them more power to work on security protection for the business with better success. Bromium says its LAVA delivers high malware detection rates. Micro-VM analysis can look at forms of attack that include rootkits and bootkits and generate signatures for otherwise undetectable attacks. The idea is that an enterprise security team can in turn update security mechanisms or fortify defenses of specific attack targets.

The drawback is that the product only works on Windows. Platform requirements in full are given as Intel i3, i5, i7 processor; 4 GB RAM; Windows 7 64-bit. It does not run on Macs and it does not run on ARM architectures.

Some outsiders say that this represents lost opportunity for the company as, on the enterprise level, more employees are using iPads and mobile devices to do their work. Nonetheless, the company co-founders have told reporters that in time wider support is in the works including versions for Windows 8 and Mac OSX. This week's product announcement had some sites voicing superlatives, implying the software can do a lot to mitigate the business angst and costs of computer malware.

More information:
www.bromium.com/
www.bromium.com/misc/Bromium_vSentry_WP.pdf