Wedge Offers Vulnerable Businesses WannaCry & Future Ransomware Threat Protection as Free Trial

WedgeAMB Uses Multiple Layers of Network Security to Detect and Immediately Block WannaCry and Future Variants of Ransomware – Providing Immediate Protection

Wedge Advanced Malware Blocker

Wedge Networks

CALGARY, ALBERTA, CANADA, May 24, 2017 /EINPresswire.com/ -- Wedge Networks, the leader in real-time network threat prevention, today announced a “Prevention First” program making virtual machine (VM) versions of the Wedge Advanced Malware Blocker™ (WedgeAMB) immediately available as free trial systems to protect enterprise networks while companies re-evaluate their threat prevention strategies. Countless businesses and institutions globally were caught off guard and unprotected by the WannaCry ransomware attack over the past week. WedgeAMB uses a unique combination of patented real-time deep content inspection with four different cutting edge security technologies to detect and immediately block new zero-day multi-vectored threats such as WannaCry ransomware and much more. For a limited time, Wedge is offering free access to WedgeAMB VMs to concerned network operators for up to 90 days, providing them with advanced threat prevention while they seek budget approvals for longer term requirements.

“Security is evolving as rapidly as new threats such as the WannaCry ransomware attacks”, said James Hamilton, CEO of Wedge Networks, Inc. “Enterprises are challenged to keep up with investigating and evaluating new security technologies to protect against brand new, never before encountered threats. They need solutions that provide immediate protection against new threats as they emerge, without having to wait hours or days for their vendor to issue a new signature or software update. WedgeAMB provides this level of new threat prevention and we want to make it available to companies with a concern about their current vulnerability to these attacks. That’s why we’ve launched the Prevention First program.”

“Computex used the recent release of the WannaCry ransomware-worm as an opportunity to validate the efficacy of the Wedge NetworksAMB solution in identifying the new WannaCry variants and sanitizing them from the network stream. The WedgeAMB appliance blocked all known variants of WannaCry as well as the worm’s proliferation efforts via the Microsoft SMB vulnerability exploit

mechanism” said Jason Robohm, Practice Manager of Cybersecurity for Computex Technology Solutions. "Our customers were not impacted by WannaCry because Computex understands the importance of cybersecurity and has always been a step ahead of the bad guys in helping protect our clients. We recommend, deploy and manage solutions like Cylance Protect and Wedge Networks for our customers. Our relentless focus on cybersecurity coupled with our disciplined approach to keep IT assets current, patched and secure powered by our Managed Services team has always yielded the great results a CISO strives for," said Faisal Bhutto, Computex VP of Enterprise Networking, Cloud, & Cybersecurity.

The WannaCry ransomware is reported to have been delivered using different threat vectors. In some cases, phishing attacks were used to deliver the ransomware payload, in other cases a worm, exploiting a vulnerability in Microsoft SMB v1.0 servers was used. WedgeAMB employs a combination of technologies which makes it uniquely positioned to defend against these multi-vectored attacks.

The 100 Mbps and 1 Gbps VM versions of WedgeAMB are available for a free download and trial period evaluation. Interested parties can register for a free trial and evaluation system by visiting www.WedgeNetworks.com or via this trial registration link.

As a VM, WedgeAMB will run on standard, commercial off the shelf server hardware which enterprise customers can procure online or from local computer stores. The VM can be loaded on a variety of virtualization hosts which are also available online. Details on the required virtualization environment can be found on the WedgeAMB data sheet.

By the end of the 90-day evaluation period, customers can convert to a fully licensed VM systems or purchase an appliance. There is no obligation to purchase a WedgeAMB license or appliance.

About WedgeAMB and Free Evaluation System

WedgeAMB™ is one of the key security application sets supported on the Wedge’s Absolute Real-time Protection (WARP) Series of network security products. WedgeAMB is available in both appliance and virtual machine (VM) versions, supporting 100 Mbps, 1 Gbps, and soon 10 Gbps network connections. WedgeAMB is typically placed in-line at the enterprise or datacenter location, where it conducts a combination of deep packet and deep content inspection, including the real-time creation of fully reconstructed MIME objects (web pages, word, PDF, power point, excel documents, etc.) and subjects them to an orchestrated, multi-thread scanning with IPS/IDS, signature-based AV, heuristic-based AV, and AI-based anti-malware. This comprehensive analysis is completed in milliseconds, allowing malware to be detected and immediately blocked at the network level, before content is delivered to endpoints. Further information on WedgeAMB is available on the Wedge Networks website, or in this link to a WedgeAMB product brochure.

WedgeAMB is based upon the same award winning Wedge security technologies and software that lead to Gartner’s inclusion of Wedge Networks in their 2016 Cool Vendor report for cyber security.

About Wedge Networks:

Wedge Networks™ is revolutionizing real-time network security with cutting edge innovation, performance, and scale. Embracing global innovation, Wedge’s Cloud Network Defense™ (WedgeCND™) and Absolute Real-Time Protection (WedgeARP™) Series of products integrate and orchestrate the industry’s highest performance security inspection and mediation engines with best-in-class security technologies developed by Wedge and third parties. Purpose-built as fully virtualized security systems, these products can be deployed in the form of x86 appliances, virtual machines, or cloud application software. Today, these industry-leading solutions block security threats for tens of

millions of end users in enterprise, service provider, government agency, and security-as-a-service networks spanning more than 17 countries.

Wedge Networks is headquartered in Calgary, Canada with international offices in Dallas, USA; and Manama, Bahrain. Visit http://www.wedgenetworks.com/ for more information

Kate Fly
Zonic Group PR
+1 512 751 4637
email us here
