BROCHURE

wedge networks
securing the cloud connected world

ABSOLUTE REAL-TIME PROTECTION SERIES™

ADVANCED MALWARE BLOCKER™

WITH CYLANCE ARTIFICIAL INTELLIGENCE

Making Threat Prevention Priority #1

Advanced threats have become so evasive that current technologies have proven to be unreliable for malware, forcing enterprise security strategies to shift from prevention to post breach detection and remediation. While detection and remediation will always be an important part of best practices, effective threat prevention is still the first order of business.

Wedge Advanced Malware Blocker™ (WedgeAMB™) is the first product in Wedge's new Absolute Real-time Protection (WedgeARP™) Series. It delivers the unique combination of industry leading threat detection and blocking accuracy with the industry's best real-time performance. This is achieved by the integration of cutting edge artificial intelligence (AI) technology from Cylance® with Wedge's patented Security Orchestrator (WedgeSO™) and other best of breed technologies to provide the industry's most effective real-time, inline malware prevention.

To further aid in sustaining effective prevention, WedgeAMB also provides WedgeIQ™ for network-wide reporting and visualization of multi-dimensional threat metrics to provide actionable threat intelligence.

WedgeAMB

"Putting Prevention back into Prevention Systems!"

Great Security Starts with Real-Time Visibility

At the heart of WedgeAMB is Wedge's patented Security Orchestrator. WedgeAMB is placed inline with the flow of traffic entering and leaving the enterprise network, data center, or partitioned sub network. As traffic flows, it inspects packets and packet payloads, and reconstructs the full file content using a combination of deep packet inspection (DPI) and deep content inspection (DCI). The content is then scanned and analyzed with a series of threat optimized virus and malware blocking engines. Real-time visibility to packets and fully reconstructed content sets the stage for accurate detection and blocking of conventional and advanced threats.

Benefits of WedgeAMB

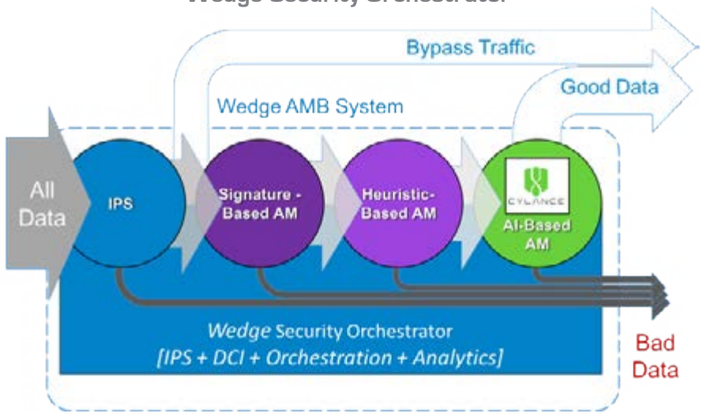
- Advanced Protection, blocking customized and unknown malware that evades real-time protection by other systems
- Protecting all endpoints, including Bring Your Own Devices (BYOD) and Internet of Things (IoT) that connects to the enterprise network
- Offloading Anti-Malware and SSL decryption from NGFW and other appliances to dramatically improve scale and performance, eliminating upgrade expense
- Supporting 100 Mbps, 1Gbps and 10 Gbps configurations deployed as VM or pre-configured appliances to satisfy diverse location requirements
- Reducing the frequency of business disruptions, and expense of dispatching threat detection and remediation teams by eliminating threats before data is delivered
- Providing overloaded security personnel with clear and actionable network-wide threat intelligence

Optimum Malware Blocking Using Multiple Layers of Detection

WedgeAMB integrates multiple best-in-class virus and malware detection technologies that are orchestrated with WedgeSO. The first step in the process is WedgeAMB's intrusion prevention system (IPS) level scanning to detect and block worms and other layer 3 threats. Next, the DCI engine is used to separate content that should be further scanned from content that will not be scanned, such as VOIP traffic, streaming video, and other "customer-defined" policies.

All remaining traffic and associated content is then scanned using Wedge's full library of more than 100 million known virus and malware signatures sourced from third party anti-malware partners. The same content is then scanned using Wedge's Heuristics detection engine to detect and block new variants of known threats. Collectively, these scans reliably detect and block more than 99% of viruses and malware that may exist in typical enterprise networks today.

Wedge Security Orchestrator



All remaining traffic is then further analyzed using artificial intelligence (AI) engines based on Cylance® predictive malware prevention. These AI engines are used to detect and block any remaining zero-days, targeted, and other advanced persistent threats that may be present. Cylance's industry leading predictive malware prevention engine combines machine learning with artificial intelligence to yield the highest real-time threat accuracy available.

Collectively, this multi-layered anti-malware approach leverages WedgeSO's single inspection and content reconstruction cycle to provide the industry's highest performance detection of both known and unknown threats, with only milliseconds of latency for a safe and satisfying network user experience.

As an option, data identified as malware by the AI engine can be forwarded to a sandbox to further characterize new malware and to reclassify any potential false positives as good data.

> "Sandboxing yields similar detection accuracy, but can require 10's of minutes to evaluate executable files.
>
> WedgeAMB detects even the most advanced threats in milliseconds, for real-time threat prevention!"

Orchestrated For Superior Scale and Performance

Over time, many vendors will boast support for artificial intelligence, but few, if any, will deliver with the performance and scale of WedgeAMB!

The magic is based on WedgeAMB's Security Orchestrator engine which leverages multiple patented technologies and trade secret techniques to deliver industry leading performance while using commercial-off-the-shelf (COTS) x86 servers. Unlike other security systems that were developed and optimized to run on proprietary ASIC or specialized FPGA-based hardware, WedgeSO was designed and optimized to run as an orchestrated virtual machine without hardware dependencies.

WedgeAMB's onboard orchestrator monitors the load and performance of each virtual network function (VNF) that is running to support the range of diverse compute activities.

As workloads increase for one set of VNFs, the orchestrator dynamically allocates more CPU resources to those functions. If workloads approach the capacity of a single VNF, the orchestrator simply spins up more VNF instances and distributes the workloads for sustained throughput. As workloads shift over time, resources are reallocated to always achieve the optimal overall system performance on any given server.
Performance gains are further achieved through a combination of optimized software architectures and code written and optimized for superior performance in massively multi-thread parallel processing environments. Patented techniques such as Wedge's SubSonic Engine™ and GreenStream™ technology use machine learning and other techniques to maximize throughput with imperceptible latency.

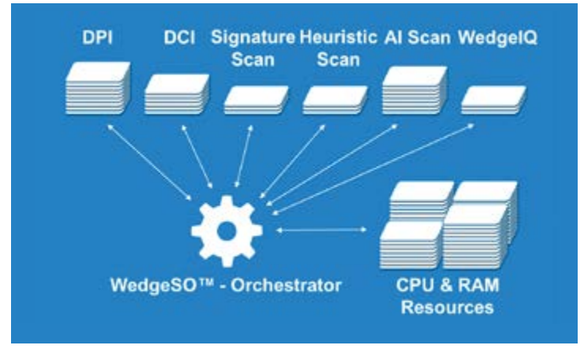
Redefining Security Scale

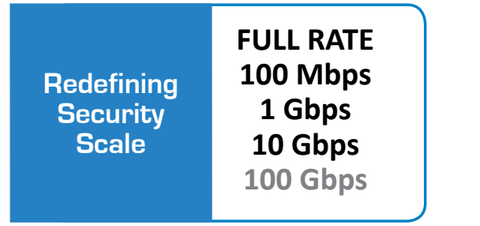
WedgeAMB is available initially in 100 Mbps, 1 Gbps, and 10 Gbps configurations, with higher speed offerings already in progress. While other vendors may offer products marketed at similar speeds, WedgeAMB is radically different in the ability to actually scale to these rated speeds, while supporting full security scanning, with SSL decryption and re-encryption.

Maximizing Deployment Flexibility

The entire series of WedgeARP products are designed and implemented using the principles of virtualization and orchestration to achieve best in class performance, without dependencies on proprietary hardware. As a result, WedgeAMB is available as a high performance virtual machine (VM) that can be run on commercial-off-the-shelf (COTS) hardware, or on a pre-configured appliance that is fully backed by Wedge with deterministic performance. This combination of packaging and scale options support optimized deployment across all locations for enterprise-wide malware prevention and network-wide threat analytics.

Orchestrated For Superior Scale and Performance





Maximizing Deployment Flexibility

Visualizing the Threat Landscape for Actionable Threat Intelligence

WedgeAMB integrates the WedgeIQ™ threat analytics and intelligence engine to provide network wide visibility into the types, quantity, origination, and targets of WedgeAMB blocked threats across the network. Threat intelligence is rolled up from each node, for analysis and visualization using advanced graphing techniques to render complex data sets as intuitive and actionable information.

Real-time visibility to the network-wide threat landscape empowers security professionals with the intelligence they need to identify and act on the most critical threats, further maximizing security.

North America 1 888 276 5356 sales@wedgenetworks.com
USA Headquarters Dallas,TX USA // +1 888 276 5356
Corporate Headquarters Calgary, AB CAN // +1 403 276 5356
APAC Headquarters Beijing, CHINA // +86 400 099 3343
www.wedgenetworks.com

wvc:20160920