DATA SHEET

wedge networks
securing the cloud connected world

ABSOLUTE REAL-TIME PROTECTION SERIES™

INTELLIGENT WEB SHIELD™

OVERVIEW

While the current SWG market has been quite strong in growth and profitability, with the changes in end-user mobility, SWGs have not seen any real improvements in both cloud-based services and defense against advanced threats. Enterprises are realizing that their SWGs need improvements with requirements for strong protection where endpoint agents are not practical, increased defences against web-borne threats, and the ability to provide stronger enforcement of acceptable web usage policies at scale for their continually growing networks. Wedge Abolute Real-time Protection™ Series (WedgeARP) – Intelligent Web Shield (IWS) is the next generation SWG that enables enterprises to upgrade their arsenals; improving protection effectiveness, supporting software defined and cloud-based networks, and providing the ability to scale to data center grade network bandwidths while securing a growing number of heterogeneous endpoint devices on their networks.

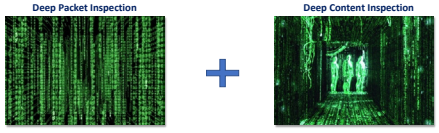
> *"Secure Web Gateways (SWGs) utilize URL filtering, Advanced Threat Defense (ATD) and malware detection to protect organizations and enforce internet policy compliance. SWGs are delivered as on-premises appliances (hardware and virtual), cloud-based services or hybrid solutions (cloud and on-premises)."*
>
> – Gartner, Hype Cycle for Threat-Facing Technologies, 2018, Pete Shoard, 13 July 2018

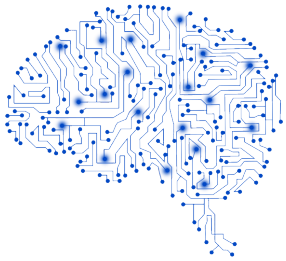
wedgeIWS
intelligent web shield

Delivering the Critical Capabilities of Secure Web Gateways

Wedge Intelligent Web Shield™ (WedgeIWS™), an offering under the Wedge Absolute Real-time Protection™ (WedgeARP™) product series, with its Advanced Malware Blocker, web filtering and Safe Search functions, is a next generation SWG. It allows enterprises to deliver the critical capabilities that their info security leaders are looking for.

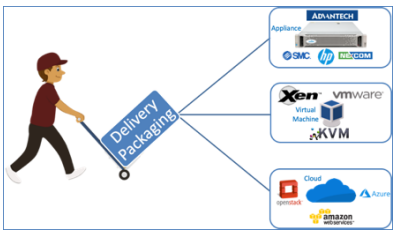
FIRST, it provides the deepest visibility into network activities with its patented Deep Content Inspection. This serves as a linchpin to insightful, actionable security analytics on the dashboards and reports of WedgeIQ™, which is a bundled big security data analytics system and policy console. In addition to web/HTTP/FTP, WedgeIWS™ supports the security of all email protocols in all deployment modes. This allows enterprises to quickly add the "must-have" robust email security solution into their networks.





SECOND, it is the most effective network security platform against ALL threats, including advanced persistent threats and new, never-before-seen malware. It utilizes multiple signature and heuristics-based scanning engines, along with an embedded deep-learning Neural Network for detecting brand-new malware in real-time. These features greatly reduce the response time and noise-to-signal ratio; eliminating the need for ineffective IDS or sandbox-based solutions. It has built in security intelligence for mobile and IoT threat prevention measures; hence offering broader security use cases for a wider range of verticals.

THIRD, WedgeIWS™ functions can be delivered as VM or appliances; on premises or in private or public clouds. This allows enterprises with the adaptability needed for more comprehensive networks and deployments and for any customer situations that they face. One of the challenges facing growing enterprises is the increasing need for mobility and BYOD support. WedgeIWS™'s centralized management of multiple systems allows security policies for the increasing numbers of endpoints to be managed on a very large scale.



wedge networks
securing the cloud connected world

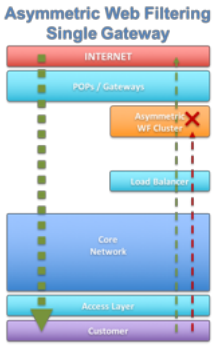
WedgeIWS Use Cases

WedgeIWS, as a next generation Secure Web Gateway, caters to the following Use Cases:

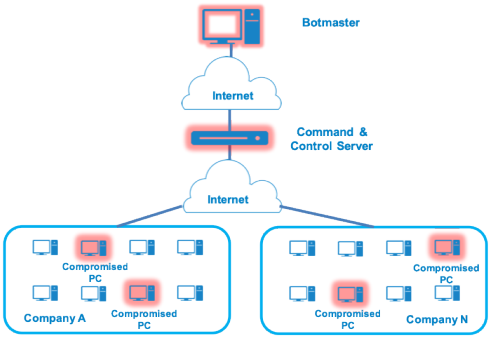
Monitoring / Visibility / Control - Business and School Web Filtering

Business and School Web Filtering enables organizations to control acceptable web usage, increasing user productivity during work / school hours, using best-of-breed web classification databases and safe search services.

With an available asymmetric web filtering mode, compliance for larger organizations and even nation-wide networks can be administered, with a reduction in solution footprint and OPEX by 90%.



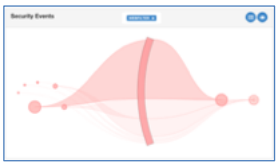
Detection of Infected Hosts



Outbound web-filter capabilities of WedgeIWS enhances network security by also giving network administrators visibility with the detection of infected hosts within their networks, allowing them to pinpoint and remediate compromised endpoints.

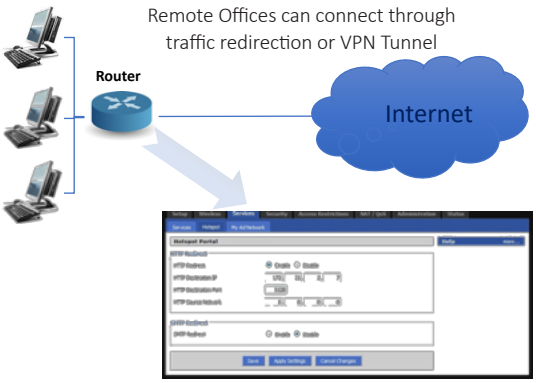
Malware Detection and Advanced Threat Defense

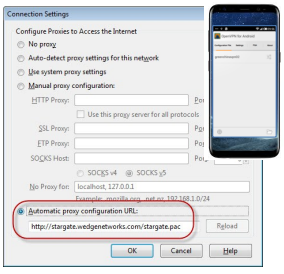
With the complete real-time detection and blocking features of WedgeAMB, organizations can defend themselves against ALL malware threats, including advanced persistent threats and never-before-seen malware. This protection is further enhanced with the optional cloud-based sandbox, WedgeMA, that can provide further insight and classification of grayware.



wedgeAMB
advanced malware blocker

Protection of Remote Offices and Mobile Workers





Having the ability to be deployed on appliance or VM; on premises or in private or public clouds, WedgeIWS can provide further protection for remote offices and mobile workers. With remote offices connecting in through traffic redirection or VPN tunnels and mobile workers accessing through HTTP(S) proxy, all of the content can be redirected to a WedgeIWS cloud for cleaning and compliance / policy administration.

North America 1 888 276 5356 sales@wedgenetworks.com Corporate Headquarters Calgary, AB CAN // +1 403 276 5356
USA Headquarters Dallas,TX USA //+1 888 276 5356