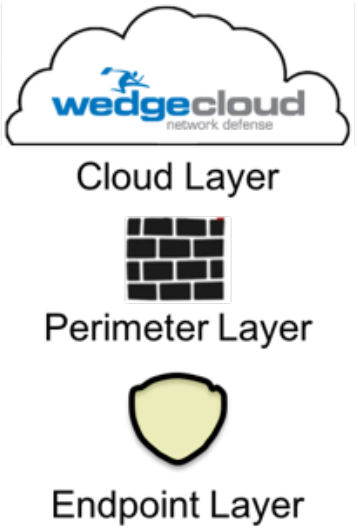
PRODUCT OVERVIEW
CLOUD NETWORK DEFENSE™

Cloud-Layer Optimized Security

The evolution and redistribution of security functions to provide network security at the cloud-layer of the network is inevitable. In tandem, the transformation of network security systems to provide these functions with cloud agility and scale is also inevitable. Wedge Cloud Network Defense™ was purpose-built to address both of these security trends and the resulting security solution requirements.

Layered Security 2.0

Nearly a decade ago, the concept of layered security was promoted as a means of using different security technologies in combination to provide more resilient security. Layered Security 2.0 expands on the concept of different logical layers for security enforcement, spanning from the cloud-layer, to the perimeter-layer, and ultimately to the endpoint-layer.

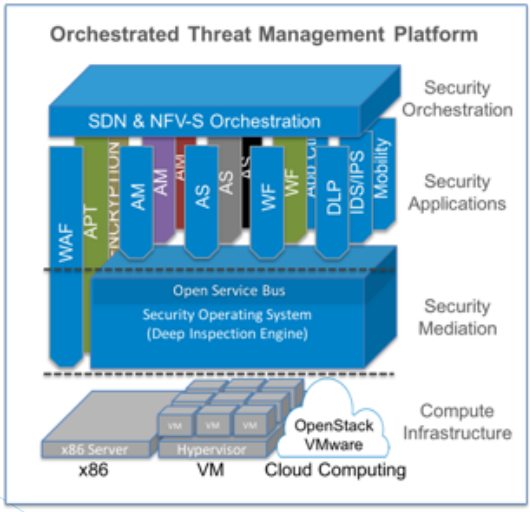


Wedge Cloud Network Defense is purpose-built for deployment at the cloud-layer, closing critical security gaps while implementing primary security functions uniformly and consistently for all users, with all devices, at all locations. For some users, nearly all of the security enforcement will be delivered from the cloud, but for others, the cloud layer will initially offload a subset of the security functions from the other layers and expand to introduce new functions over time.

Cloud-Layer Implications For Scale

For larger enterprises with their own cloud, implementing security at the cloud-layer of the network will result in the roll up of traffic across multiple regional enterprise locations into one data center. Smaller businesses that do not have their own cloud will look to their communications service provider (CSP) or other cloud access security provider to implement their cloud-layer of security-as-a-service, and these services will be extended to large numbers of businesses.

In both scenarios, the connectivity of business locations to this data center will increasingly use new software-defined wide area network (SD-WAN) services to dynamically provision incremental bandwidth on-demand to support peak activity workloads. Collectively, these conditions indicate that cloud-layer security platforms must be designed to support dramatically greater scale and a more variable dynamic range of traffic loads than is supported by today's conventional security appliances.



Cloud Optimized Platform Architecture

Data centers are rapidly evolving to use software-defined network (SDN) technologies with network functions virtualization (NFV) and orchestration to achieve cloud efficiency, agility, and scale. Wedge Cloud Network Defense was architected and implemented using these same concepts to provide a revolutionary Orchestrated Threat Management (OTM) platform architecture. The result is a software-defined security platform that can be implemented on a commercial off the shelf (COTS) x86 server, as virtual machine, or in an elastic cloud-compute environment using OpenStack, VMware or other cloud virtualization software for unlimited computing scale.

wedge networks

securing the cloud connected world

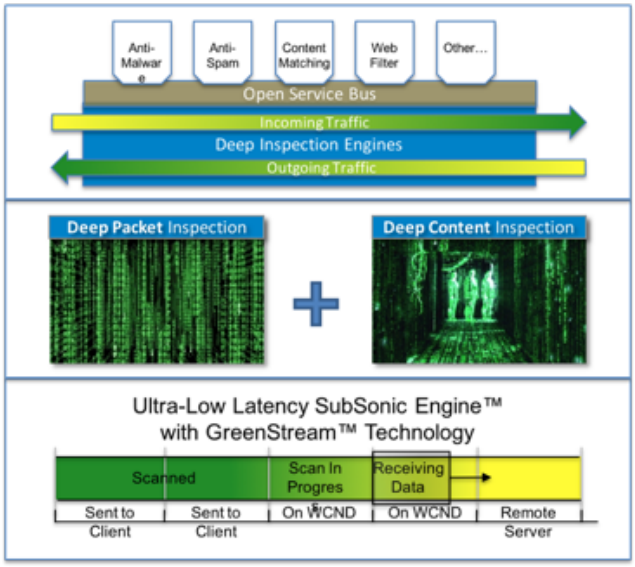
At the core of Cloud Network Defense is WedgeOS™, a deep inspection security mediation engine. WedgeOS combines Deep Packet Inspection (DPI) with Wedge's patented Deep Content Inspection (DCI) to scan both packets and content that is distributed across multiple packets. Content is reconstructed and then analyzed through Wedge's Open Service Bus using one or more of over a dozen different security virtual network functions (VNFs) developed by Wedge and third party vendors. The Cloud Network Defense Orchestrator facilitates service chaining of these WedgeOS VNFs and standalone third party security VNFs to support a range of security policies that are uniquely enforced based on the identity of the packet.

Cloud Network Defense is the industry first OTM platform, yielding dramatic advantages in security scale, elasticity, automation, and agility, with multi-vendor support, and hardware independence.

Cloud Optimized Performance

Cloud Network Defense's support of the Open Service Bus, enables multiple entire libraries, each consisting of 10's of million threat signatures, to be scanned along with heuristic analysis and sandboxing of deeply inspected content to provide greater threat detection accuracy than any known security appliance.

Cloud Network Defense sits inline with the flow of traffic, so all scanning must be completed with imperceptible latency or application performance will degrade, along with customer satisfaction. The WedgeOS security mediation engine implements multiple patented processing techniques such as GreenStream™, which enables the scanning of very large files without the conventional constraint of holding all packets until the entire file scan is complete. Additionally, Wedge's patented SubSonic Engine™ uses elastic compute scale in combination with multi-threading technology and advanced computational techniques to achieve sustained low latency (typically single digit milliseconds) throughput, regardless of traffic scale.



Cloud Network Defense security software was written using a multi-thread coding technique to optimize performance for multi-core CPU cloud compute environments. This coding technique further contributes to optimal performance. Collectively, WedgeOS' security mediation engine has demonstrated 20x to 30x faster throughput than competing systems and is a proven security engine securing more than 80 million endpoint connections word wide.

Flexible Services Scope

The software-defined nature of Cloud Network Defense positions it as the ideal platform for a phased and flexible migration of security functions to the cloud. As a software application that can run on the cloud, it can be configured to provide a minimal subset of security services, such as offloading web filtering, anti-malware and anti-spam functions from an existing UTM or NGFW to close critical gaps for secure web gateway (SWG) and email security (ES) services. Data loss prevention (DLP) services can be activated at anytime to enable more advanced threat protection (APT). Application control can be activated to consistently limit the use and bandwidth allocation to certain non-business related applications. In total, more than a dozen different security VNFs are available to support a wide variety of security applications.

Flexible Licensing Models

Enterprise customers can simply purchase the applications licenses based on desired functionality and scale. For CSPs, Wedge also offers flexible Pay-as-you-Sell security-as-a-service subscription licenses which enables CSPs to Wedge-enable your entire network and pay nothing for the software until you actually sign up customers. Running Cloud Network Defense on existing cloud resources eliminates the need to procure dedicated hardware, while deferring license fees until subscribers subscribe, is the perfect model for CSPs to expand into the rapidly growing and lucrative security-as-a-service market.

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
APAC Headquarters Beijing, CHINA // +86 400 099 3343
www.wedgenetworks.com