| DATASHEET

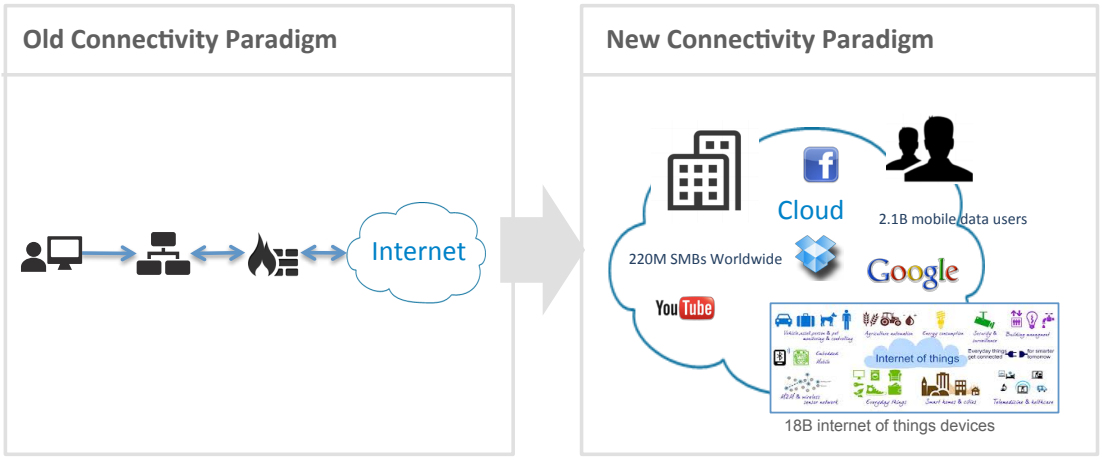
wedge networks
securing the cloud connected world

CLOUD NETWORK DEFENSE™

POWERED BY WEDGEOS™

Overview - Cloud is the new Edge

Mobility, cloud, consumerization of IT and Internet of things have completely redefined how we consume and access information while also introducing a new generation of threats. The result is a new connectivity paradigm where the cloud is now the center of the world's connected networks and the security challenge is now how to secure this cloud-connected world, given that most of the current security solutions are either end-point or perimeter based.



The technology that defines a communications network is changing rapidly too. Major innovations enable new possibilities to deliver a network as a flexible, scalable and versatile service, free of vertically integrated hardware appliances and physical network routing.

Wedge's Cloud Network Defense™ (CND) transforms how security is delivered today. It is an infinitely scalable Security-as-a-Service (SECaaS) platform run in the cloud. This platform leverages Software Defined Networks for Security (SDN-S) and Network Functions Virtualization for Security (NFV-S) technology to embed security as a scalable, high performance service in today's cloud connected networks. By enforcing unified web, email and mobile security policy across all network traffic, all devices are protected - anytime, anywhere.

Most network security technologies rely on proprietary hardware such as ASIC. Wedge's key value-adds are found in its software innovations. Current Cloud Security providers direct traffic to their 3rd party infrastructure for inspection, causing delays or latency. Together with its patented Deep Content Inspection (DCI) Engine and Deep Packet Inspection (DPI) Engine, Cloud Network Defense™ utilizes advanced software to direct and load-balance computing resource usage. This includes adding and removing instances as required, which is not easily carried out on hardware-based platforms. CND provides comprehensive security, in real-time, without requiring traffic to leave the network. The Wedge approach takes advantage of cloud computing architecture which offers scalability, elasticity (dynamic reallocation per demand), ubiquitous availability, and high capacity for the cloud centric networks of today and into the future.

wedgecloud
network defense

Highlights: Security-as-a-Service (SECaaS)

- **Elastic Security Services Orchestration™** integrates SDN, NFV & cloud management capabilities to dynamically process high volumes of network traffic in real time without compromising the performance of the world's largest networks
- **Embedded security** inspects and applies policies without requiring traffic to leave the network
- **Exhaustive content inspection** of all inbound and outbound traffic to defend devices, users, data and web applications
- **Open platform** delivers interoperability with different identity management programs, OSS systems, cloud orchestration systems, SDN controllers and network components
- Support for standards-based cloud management and virtualization technologies such as OpenStack and KVM
- Intuitive user interface, a single-pane-of-glass for managing all elastic security services

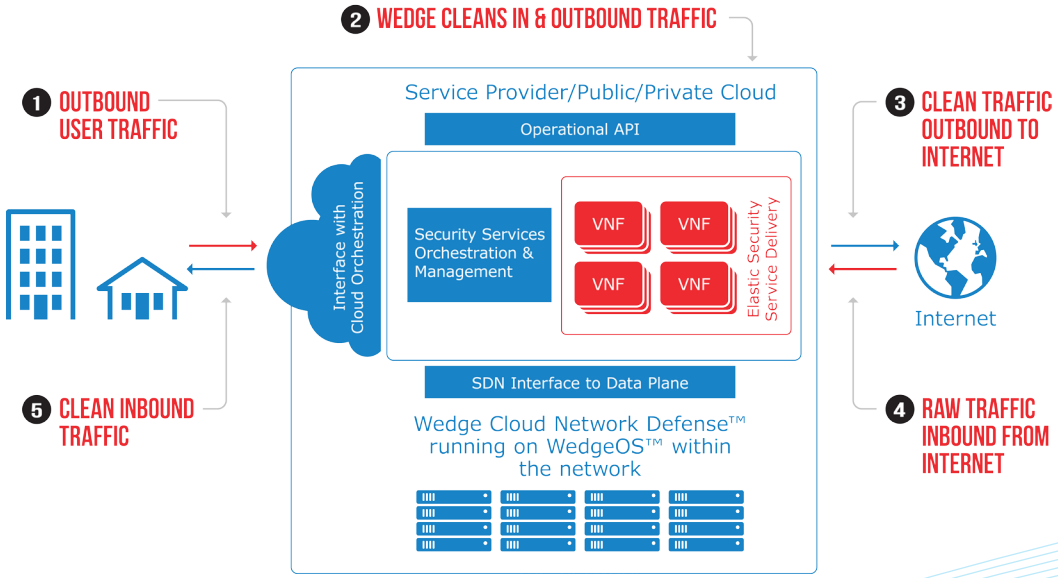
How Cloud Network Defense™ Works

Cloud Network Defense™ receives user policy and endpoint identification from a number of sources, depending on how it is deployed. Identity Management System, Telco OSS/BSS, or registration via a Portal are some examples of this.

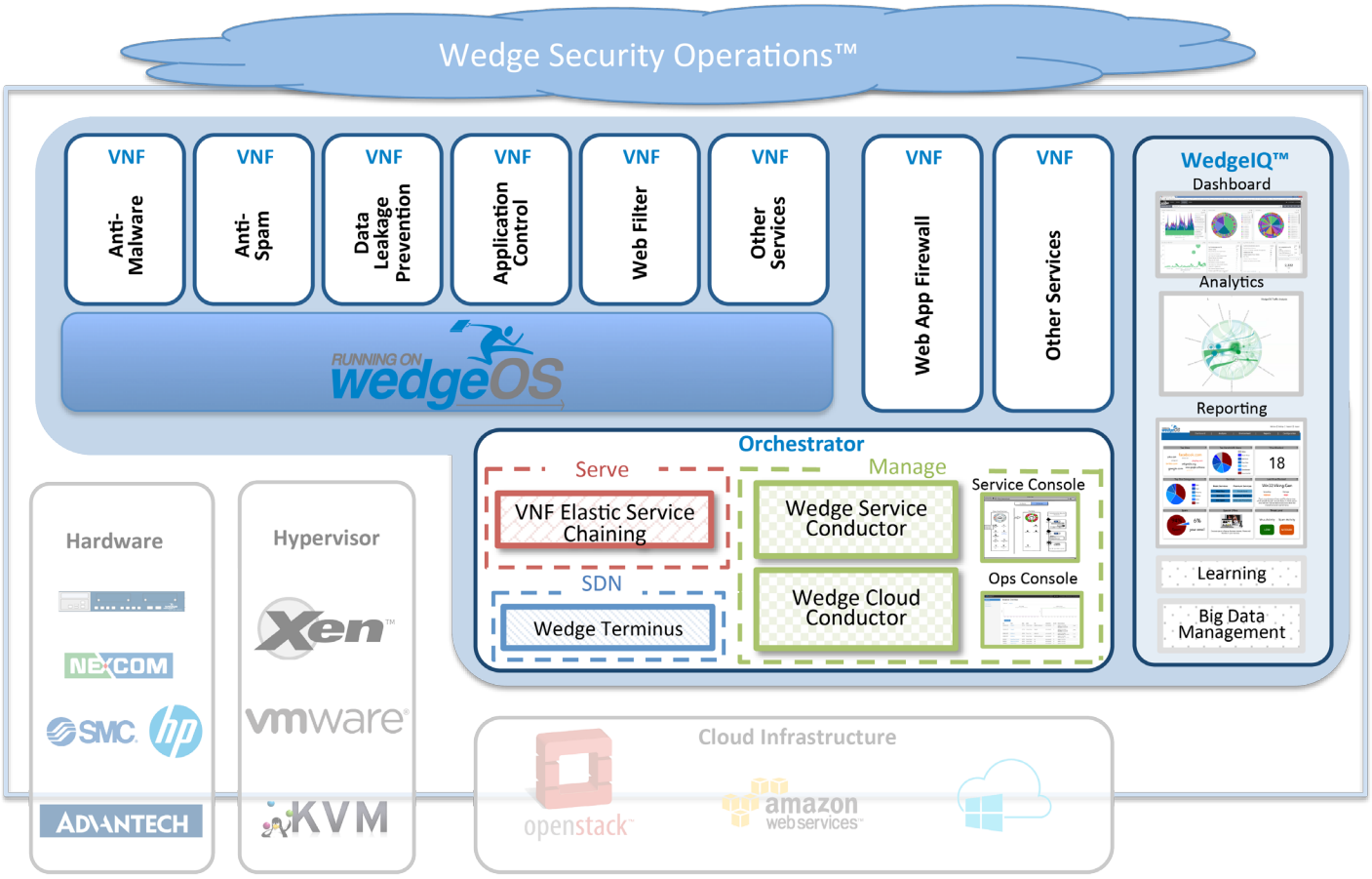
The system then uses that information to control the network flow to inspect and enforce security policies to selected network traffic through its network function virtualization for security (NFV-S) compute stack.

The network function virtualization for security is the foundation of Wedge Cloud Network Defense's™ Elastic Security Service Orchestration. Working as a pooled resource, it dynamically applies specific policy-based security inspection to specific user device traffic in response to network load. It is powered by Wedge Networks' patented WedgeOS™, which is an embedded operating system that enables the delivery of a variety of security functions as an agnostic, open, and easily consumable service.

The Wedge Cloud Network Defense™ Cloud Conductor coordinates all the cloud operational aspects to dynamically monitor and maintain virtual instances and to effectively apply platform resources.



Cloud Network Defense™ Architecture



Cloud Network Defense Components

Wedge Cloud Network Defense™ containts a variety of Networking, Orchestration and Management Components. These include:

Wedge Security Virtual Network Functions (VNFs)

Wedge VNFs are components of Wedge Cloud Network Defense™ that handle specific network security functions such as Anti-Malware, Anti-Spam, DLP, and other functions such as Web Application Firewall.

WedgeIQ™

WedgeIQ™ is a powerful platform where results and statistics that are generated by Wedge VNFs are reported, visualized, analyzed, and monitored. It provides reports on blocked web attacks, spam counts, traffic usage, blocked viruses, and many more categories. The dashboard displays a comprehensive and detailed visualization of the scanning results from Wedge VNFs. It also provides the latest technology in data science by featuring data management, data analysis, and forensics.

Cloud Controller

The Cloud Controller is based on OpenStack technology and provides the following:

- Repository of virtual instances and an API to query and control these instances in the virtualized solution. The virtual instances are WedgeOS™, Wedge Cloud Conductor™, Wedge SDN Terminus™, and Wedge Service Conductor™.
- Repository of virtual images required for Wedge Cloud Network Defense™ operation. Images can include WedgeOS™ and Ubuntu.
- Creation of multiple virtual networks with IP/subnet allocations for software-defined networking.

Wedge Cloud Conductor™

The Cloud Conductor provides health monitoring of virtual instances, creates and destroys NFV-S instances based on the inspection load. It provides management of the VNF instances, SDN Terminus, and OpenFlow Switch configuration. It also co-ordinates cloud computing abilities with a single instance controlling all cloud computing operations.

Wedge Service Conductor™

The Service Conductor contains the following components:

- Service handlers distribute policies that contain subscriber information to the SDN Terminus to identify endpoint user traffic to be processed by VNFs.
- The REST API, which manages subscriber registration and policy management.
- The Security Intelligence update service, which manages user security policy configuration and identity management.
- The Policy database that contains registered subscribers and service policies for the subscribers.
- The centralized logging of security events from virtualized network function instances.

Wedge SDN Terminus™

The SDN Terminus receives subscriber policy and endpoint identification from the Service Conductor. It receives VNFinstance accounting from the Cloud Conductor and controls the data plane to flow network traffic to the appropriate VNF instance for security inspection.

VNF Elastic Service Chaining™

A feature of Wedge Cloud Network Defense™ where requests are logically sent to go through a “chain” of VNF services such as web application firewall or WedgeOS™.

Service Console

A reference self-service customer portal that can be used to register and enable security scanning services to protect endpoints that connects to Wedge Cloud Network Defense™.

Ops Console

The Cloud Conductor dashboard provides health monitoring of virtual instances and creates and destroys VNF instances based on the inspection load (i.e. Elastic Scaling). This console provides management of the VNF instances, SDN Terminus, and OpenFlow Switch configuration and co-ordinates cloud computing abilities.

Wedge Security VNFs

Cloud Network Defense™ implements unified web, email, and mobile security embedded as scalable, high performance security apps. Simple, fine-granularity policy orchestration enables comprehensive, yet non-intrusive, inspection of desired user traffic across networks of any scale. Cloud architecture enables easy provisioning of services for users with changes applied across the platform instantly.

Web Security

Cloud Network Defense's™ layered security architecture combines Deep Content Inspection, inline-anti-malware, URL filtering and behavioural analytics for complete network traffic security.

URL Filtering
Cloud Network Defense™ enables organizations to effectively manage risk by controlling access to web content across users, groups, devices and locations. URLs are filtered by global reputation against more than 280 million top-level domains spanning over 95 categories. Users can set parameters such as time interval, special categories (PCI, XSS, SQL attacks) and key word patterns.

Anti-Malware
Leveraging best of breed AV signatures, Cloud Network Defense™ applies inline Anti-Malware to network traffic with Deep Content Inspection to prevent a wide array of attacks, like:

- Advanced Threats
- Trojans
- Zero Hour
- Malware
- Viruses
- Spyware
- Malicious Apps
- Web Threats
- Worms
- Targeted Attacks
- Key Loggers
- Rootkits
- Bots
- Blended Attacks

Advanced Threat Protection
Cloud Network Defense™ is multi-vectored and understands the intent of a "threat" by following all of the users' traffic sessions across all applications / protocols. Through content recognition learning takes place across a users' sessions and protection is provided against security threats in real time.

Zero Day / Custom Malware Detection
Cloud Network Defense™ utilizes pattern matching, heuristic analysis and sandboxing to detect malicious intent in the MIME objects within the traffic streams. By using these techniques and executing suspicious binary files in a sandbox, malicious content can be identified, even if the sample has never been previously observed.

Log Output Service
Cloud Network Defense™ seamlessly transmits event logs to your SIEM in real time in a variety of log formats.

Email Security

Cloud Network Defense™ combines real-time intelligence of over 2 billion sensors worldwide with behavioural analysis and Deep Content Inspection to secure against all messaging threats.

- A complete solution to combat viruses, spam, IP blacklisting, spyware, phishing, message abuse, DDoS, advanced threats and data loss
- Stops blended, multi-channel messaging attacks with a fully integrated solution over all web and email protocols
- Secures inbound and outbound email communication
- Email policy follows mobile users regardless of location
- Suspicious/Infected emails automatically quarantined
- Only transparent (non-MTA) two-way messaging security solution rapidly deploys into the most complex networks and data centers
- Prevent email-based data loss across all devices

DLP

Cloud Network Defense™ integrates DLP for data in motion across Web, Email, and Mobile Security, creating a defensive boundary around your critical data. Cloud Network Defense™ DLP covers smartphones, tablets, and laptops - all with a single, global policy. Inline enforcement inspects and protects both clear and encrypted content.

- With the largest coverage of file formats and protocols for inspection across over 400+ file types and multiple protocols, Cloud Network Defense™ can see and understand more than any other solution on the market.
- Highest accuracy with two-staged scan rapidly scanning streams and extracting suspicious content in linear time for more comprehensive evaluation logic, thus minimizing latencies.
- Lower TCO for protecting unstructured data (i.e. corporate IP) by not relying on high cost re-classification of your data.
- Built-in compliance support enables easy monitoring and enforcement compliance based on pre-loaded policies and reports.

Secures Data in All Applications

Web	HTML5
Games	Email
Mobile Apps	Social Networking
SMS/MMS	Mobile Payments
App Stores	Content on Demand

Mobile Security

Cloud Network Defense™ enables the secure usage of mobile devices, solving the issues of phishing, malware, network abuse, blended attacks within your network, or while roaming.

- By sending all mobile traffic - browser and application - through the Cloud Network Defense™ platform and inspecting it in real time, this protects against malicious apps, browser exploits, cross-site scripting, phishing and other advanced threats.
- Eliminate malicious attacks before they reach mobile devices with no impact on mobile functionality.
- With full content scanning and inspection across all protocols, Cloud Network Defense™ provides complete protection against third-party services or applications, including both web-based services such as Gmail, and consumer applications such as Facebook and YouTube.

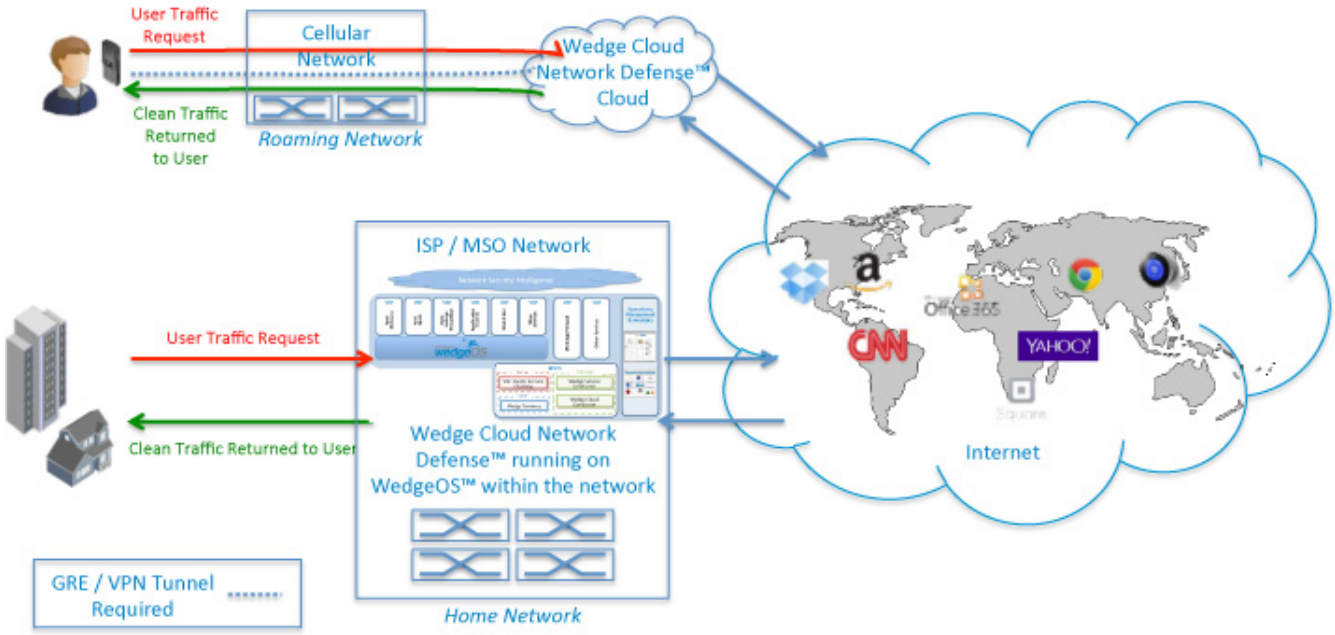
How WedgeIQ™ Works

WedgeIQ™ offers the most comprehensive real time security intelligence, allowing for the most updated and accurate protection for all endpoints. Enhanced intelligence is provided where the WedgeIQ™ security intelligence engine assimilates attack intelligence from Wedge's global technology base and creates a continuous feedback loop to protect against known and unknown threats. It combines user reputation, analysis and intelligence from SubSonic™, and various signature databases, to derive a verdict on the safety of network traffic to ensure security and compliance.

Subscribers Serviced By Cloud Networks Defense™

Subscriber computing devices serviced by Wedge Cloud Network Defense™ (CND) are protected when “in-network” or “off-network”. Home and business users have their devices’ traffic scanned and protected when serviced directly by the ISP/MSO Network. Mobile users on cellular networks without CND integration tunnel their devices’ traffic to the nearest Cloud Network Defense™ Cloud for seamless protection. In addition, subscriber devices can also be protected through the integration of Cloud Network Defense™ in both Private and Public Cloud deployments (described in the next section).

How Cloud Network Defense™ Works



Cloud Networks Defense™ Deployment Options

Being a software-based platform, Wedge Cloud Network Defense™ can be easily deployed in different scenarios. Although the typical deployment is a Service Provider Cloud where Cloud Network Defense™ (CND) is integrated within the ISP / MSO networks, CND can also be used to provide security from Private Clouds as well as from Public Clouds.

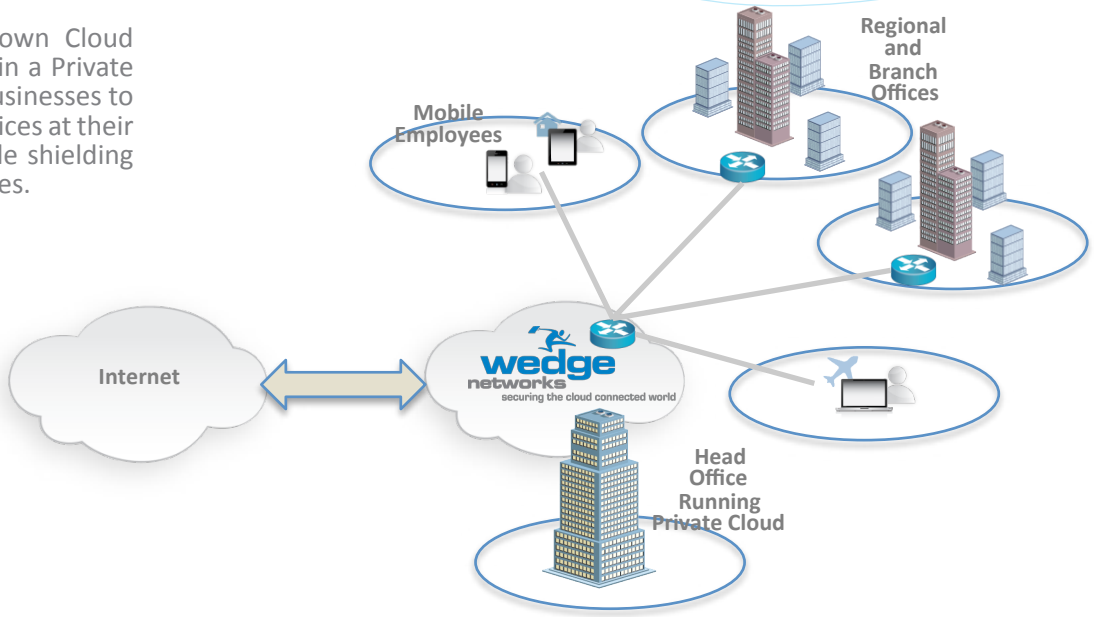
Cloud Network Defense™ Integrated into Service Provider Network

Security from a Service Provider Cloud

Integration of Cloud Network Defense™ at the ISP / MSO level allows cleaning of all data traffic inline, without the subscriber traffic leaving the operator’s network. Subscribers to the security services at the Service Provider level can be assured of total security while having the convenience of all traffic coming into their home or business being cleaned straight from their data pipe. All security integration is taken care of by the service provider.

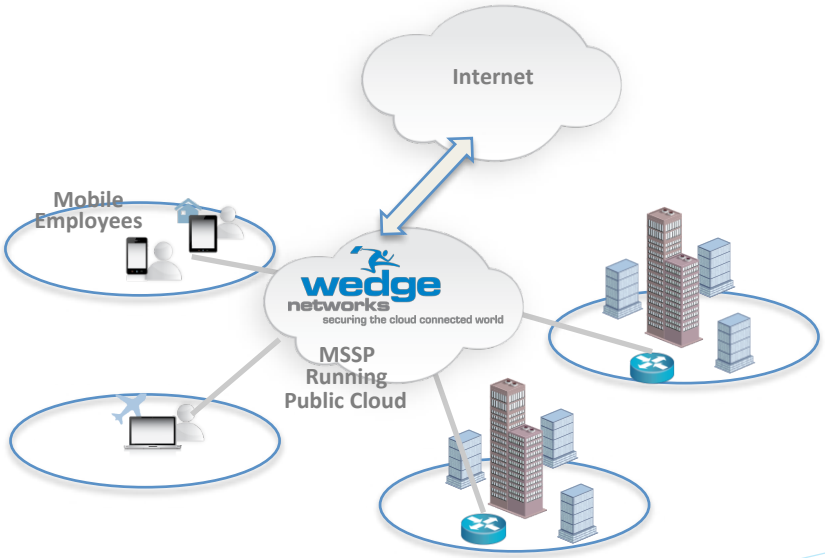
Security from a Private Cloud

Businesses can host their own Cloud Network Defense™ running in a Private Cloud. This enables these businesses to protect their employees' devices at their offices and on the road while shielding their data from outside parties.

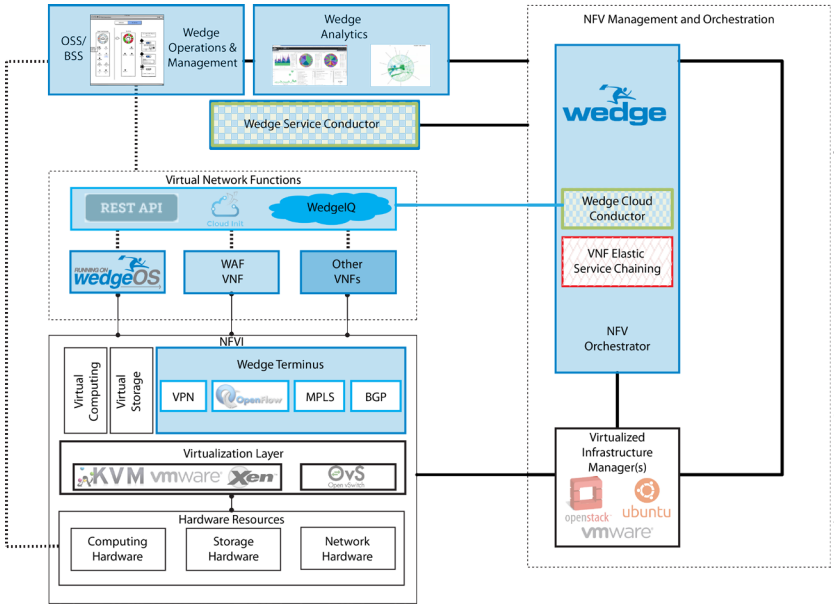


Security from a Public Cloud

In cases where businesses prefer not to host their own private cloud, perhaps due to resource constraints, in order to protect their users' devices, security can be provided from Public Clouds. Public Clouds such as Managed Security Service Providers (MSSPs), who host security services from their own cloud and who offer Security as part of their business, would offer Cloud Network Defense™ services as a white-labeled security offering.



System Requirements and Deployment



NFV Reference Architecture with Cloud Network Defense™

Openstack Environment:
Juno (or higher)

3 (or more) physical servers to act as:
- Cloud Controller
- VM Hosting Compute Nodes

Minimum Server Requirements:
8 cores, 16GB RAM, 3x 1GB NIC, 250GB HD

Software Requirements:
KVM, Ubuntu 14.04

1 Ethernet port to be on management subnet able to access the internet for package download

OpenFlow 1.1 capable switch; or compute node installed as OpenFlow capable virtual switch (OpenVswitch)

Network integration to the data plane to be protected via the options such as inline, policy-based routing, or tunneled client/server network connection to OpenFlow switch.

KVM or VMware VNF System Environments:
VM configured with the following:

CPU	2, 4 Core
RAM	4, 8 GB
Virtual Disk	16, 32 GB

About Wedge

Wedge Networks™ is transforming the way security is delivered. Powered by the innovative WedgeOS™, Wedge Networks' Cloud Network Defense™ is an orchestrated threat management platform designed to combat the shifting threat landscape associated with cloud, mobility, bring your own device, Internet of Things and consumerization of IT. By applying security policies at the cloud-layer, enterprises and network operators offering security-as-a-service can achieve more effective security, using best-in-class multi-vendor technologies, with greater efficiency and scale. The award winning Wedge Platform™ is deployed globally, delivering security protection for tens of millions of users in Fortune 500 companies, government agencies, internet and broadband service providers, and across all industry verticals. Wedge Networks is headquartered in Calgary, Canada and has international offices in Dallas, USA; Beijing, China; and Manama, Bahrain.

RUNNING ON wedgeOS

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