ORCHESTRATED THREAT MANAGEMENT: A NEW PARADIGM IN CYBER SECURITY

Synchronizing Security with Real-Time Next Generation Networks

7/25/2016 1.0.0

Contributed by Wedge Networks, Inc.

Whitepaper

Version OTM-WP-v1.0.0

Trademarks

Cloud Network Defense is a pending Trademark of Wedge Networks. Other product and company names used in this document are used for identification purposes only, may be trademarks of other companies, and are the property of their respective owners.

WedgeOS™ and associated software are protected by, or for use under, one or more of the following U.S. provisional Patents: 60/521,551, 60/522,513.

Regulatory Compliance

FCC Class A Part 15 CSA/CUS

For technical support, please visit http://www.wedgenetworks.com/

Send information about errors or omissions in this document or any Wedge Networks marketing documentation to marketing@wedgenetworks.com.

ABSTRACT

Enterprise data storage, computing, and more recently networks are evolving, becoming virtualized, software-defined, and dynamically configured, or orchestrated, eliminating the static boundaries and tangible attributes that once defined the enterprise and enterprise resources. These changes enable powerful new business opportunities with compelling economics. They also introduce new challenges and new opportunities for securing the enterprise; the problem of malware detection is increasingly difficult for many companies to solve as the organization perimeter moves. Mobile access and the emergence of new threat actors has moved most organization cyber perimeters. Further adding to the challenges is the need to maintain real-time communications over these varying networks.

Traditional cyber security platforms need to evolve to address the challenges now faced in next generation networks. New cyber security tools need to: 1) be able to capture data in motion with no queueing, 2) have full visibility of Layer 3-7 data content, 3) be able to apply multiple security policies efficiently to the content with no latency induced reprocessing, 4) identify anomalous activities with a high degree of accuracy including zero day threats and 5) capture and provide usable analytics that can quickly assist those monitoring to recognize the anomalous activities as well as assist in the machine learning of the system to improve efficiency.

Wedge Networks' Cloud Network Defense Orchestrated Threat Management (OTM) represents a progression in network security evolution, and a compelling new approach for synchronizing security with today's more open, agile, and orchestrated real-time networks and IT infrastructures. It supports virtually unlimited scale, while providing in-depth event reporting and archiving, along with analytical dashboards that can assist with improving the cyber situational awareness. Wedge Networks' Cloud Networks Defense delivers the industry's most robust deep data inspection engines, with best of breed threat security intelligence, and actionable analytics on an elastic environment enabled with event service chaining for an effective and adaptive cyber defense. This white paper explores the capabilities enabled by the Wedge Networks' Platform.

1 Introduction: A New Security Paradigm

The purpose of this paper is to describe a new, cloud-based, security paradigm that can encompass the extended enterprise, inclusive of mobile devices, BYOD, IoT, public and hybrid clouds, and dynamically provisioned network resources. This new cloud-based layer of network security subsumes many of the enterprise perimeter security functions of NGFWs or UTM appliances. Examples include: anti-spam (AS), anti-malware (AM), URL filtering, web filtering (WF), data loss prevention (DLP), application control (AC), intrusion detection/ prevention systems (IDS/IPS), web access firewalls (WAF), DDoS mitigation and more. Applying these functions at the cloud layer closes critical security gaps and provides the opportunity to implement these functions in a cloud environment, for more open, agile and orchestrated real-time network security, with virtually unlimited scale. It also creates the opportunity for premises-based appliances to be refocused on perimeter-centric security functions that are well within the scale of those appliances. The new security paradigm is an Orchestrated Threat Management (OTM) approach as delivered from Wedge Networks' Cloud Network Defense.

2 Orchestrated Threat Management

The goal of Orchestrated Threat Management is to implement NGFW or UTM type functions using a cloud-based, software-defined and orchestrated platform architecture for superior scalability, operational agility, and adaptability. The concept of OTM is to replace the closed (proprietary hardware with imbedded proprietary

software), inflexible, hardware-defined, single-vendor product attributes of the past appliances (Figure 1) with

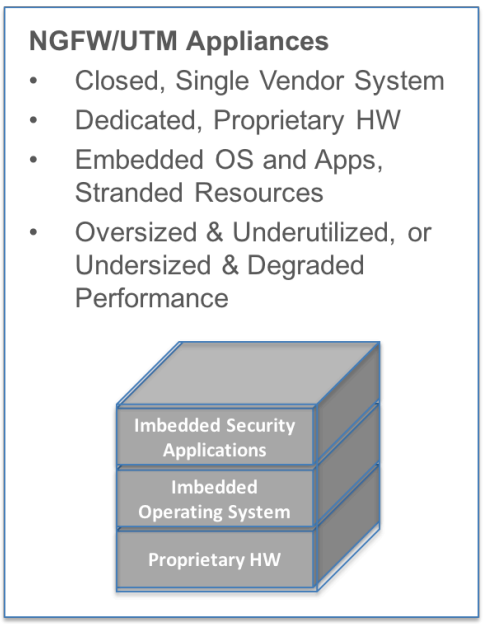

Figure 1) Traditional UTM Appliance Architecture

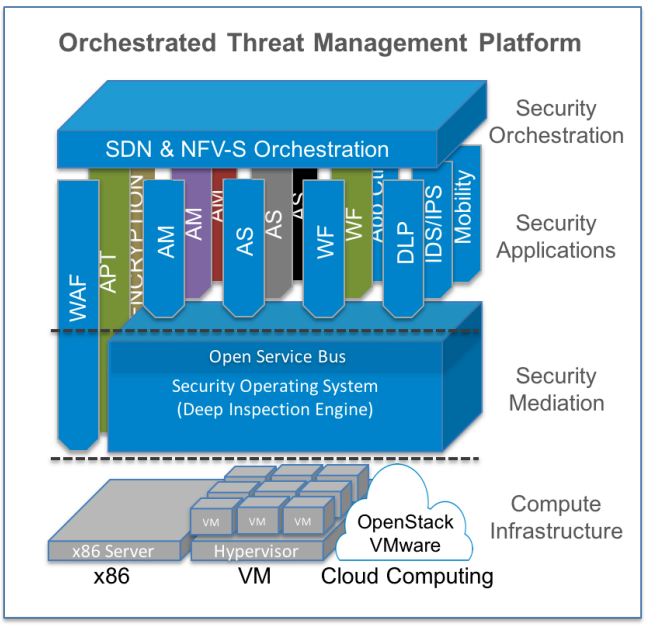

Figure 2) Orchestrated Threat Management Platform Architecture

the centrally managed, open, agile, software-defined, multi-vendor attributes of today's rapidly evolving data centers and networks (Figure 2).

Let's consider OTM further by reviewing each of the architectural layers.

2.1 Compute Infrastructure Layer

OTM platforms eliminate the dependency on proprietary hardware and the need to purchase oversized hardware appliances in pursuit of solution longevity. OTM's decoupling of software from hardware provides multiple degrees of freedom for the hardware compute layer. For example, the software may be deployed as an appliance running on a generic x86 server, using commercial-off-the-shelf (COTS) hardware; or deployed as a virtual appliance, running on a virtual machine (VM); or ideally deployed in a cloud compute environment controlled by a cloud management system such as OpenStack or VMware.

In the case of an x86-based COTS appliance, the software can be transferred to a different x86 server with more compute power and higher speed network interfaces as traffic loads increase and require more capacity. The former x86 server can then be redeployed for other applications that can be supported within its capabilities. This approach allows customers to purchase their own server hardware and eliminates the legacy appliance issue of stranded hardware and software when the capacity or performance requirements of proprietary appliance are exceeded.

In the case of a VM, the software can be loaded on a virtual machine running VMware, KVM or other virtualization operating system. This provides the flexibility to run more than one virtual machine on a server for the benefits of avoiding the purchase and installation of a separate dedicated server. One caveat for consideration with a VM is that a portion of the server's memory and compute power is allocated to the overhead associated with creating and sustaining each virtual machine. Additionally, other VMs running on the server also consume resources. So system performance can be a consideration if the server is heavily loaded.

However, it can be an ideal approach in many use cases, both in the data center and at a customer's premises. In the future, the use of a container technology such as Docker, and LXC will reduce this issue.

Within a cloud computing environment, OTM implementation is the ideal compute infrastructure. Cloud computing provides the option to dynamically spin up more virtual machines across a virtually unlimited number of servers for nearly unlimited scalability. As OTM compute requirements increase over time or possibly surge, such as in the case of a denial of service (DOS) attack, more VMs can be dynamically spun up and allocated. As requirements decrease (i.e., following a DOS attack) the VMs can be spun back down and made available for other applications running in the same cloud environment. This dynamic scalability assures that OTM performance is not constrained by statically defined system capabilities. It also delivers powerful economics when compared against the purchase and deployment of dedicated appliance hardware that must be oversized to support peak demands.

2.2 Security Mediation Layer

The security mediation layer provides the core OTM operating system, system administration, resource management, and security mediation services for the OTM platform. One of the key OTM attributes of this layer includes the ability to conduct primary security mediation functions such as opening packets for inspection and possibly reconstructing content for inspection and applying one or more security functions to the available content. Another key attribute of OTM is the support for an open service bus to allow one or more security applications, developed by one or more vendors, to plug in and apply security functions to the inspected packets and/or content.

In some cases, certain primary security functions, SSL decryption and encryption, reporting and other primary system functions may be included as part of the security mediation layer. However, in general, a variety of security functions should be available in the form of individual applications so that customers may select and apply different functions based on their individual and application specific needs. This framework will also provide the ability for security applications and technologies developed by multiple vendors to be available, giving customers more freedom and choice in selecting from a range of security applications and changing them as required over time.

2.3 Security Applications Layer

A core attribute of OTM is that applications are developed independent of the security mediation layer and easily added or removed based on customer preference. Ideally, the industry will specify a standard interface allowing any third party security application developer to create their own application and make it available for use within any vendor's OTM system. However, at this time no such industry standard has been established. In the interim, visionary market innovators such as Wedge Networks have developed their own API so they can systematically adapt security technologies from third party vendors into OTM compatible applications. By doing so, these applications can apply security functions to the packets and content that are already being inspected at the security mediation layer. This inspect once and expose to multiple applications model minimizes the latency associated with conducting the inspection process for each application and minimizes compute resource requirements.

In some instances, it may be more practical for third party applications to operate as a standalone virtual network function (VNF) that runs independent of the security mediation layer. Of course this application will need to be controlled by the security orchestration layer to be considered as part of the OTM. Otherwise it

would simply be an independent security VNF. Possible examples of this form of implementation include Web Application Firewalls (WAF), Sandboxing, and packet level Encryption.

The primary benefits of disaggregating applications via OTM is the ability for applications to evolve independently of the security mediation and orchestration layers, to be developed by third parties, and to easily be introduced or removed from the OTM configuration as required.

2.3.1 Deep Learning for Improved Security Application Identification of Zero Day Threat

Within an OTM, security against malware is a priority cyber security application. The ability of the OTM to systematically adapt new security technologies enables the OTM to evolve the offered cyber protection as newer methodologies for malware identification become available. Moreover, the ability of the OTM to orchestrate multiple third party security applications to be orchestrated together provides the ability to adopt new emerging methods of malware identification while still leveraging current proven methods.

Within the Wedge Networks' OTM, deep learning has been incorporated with industry best of breed signature and heuristic-based methods to provide the first cloud based artificial neural network (ANN) implementation of malware detection that is not only highly accurate but processed in real-time. Additionally, the Wedge Networks OTM utilizes machine learning to improve malware detection in that:

- the patented Subsonic DCI engine allows the rapid propagation of "learned" intelligence to other WedgeOS systems, hence enhancing the immune system of the whole network.
- the WedgeOS and related third-party VNFs have the ability to gather contextual data from L3-L7 for Big Data acquisition, storage, and indexing. The WedgeIQ uses a distributed data storage architecture allowing archival and indexing the data set in real-time; and
- the WedgeIQ uses advanced data visualization technology to effectively communicate the relationship of the elements in a threat domain to human analysts with improved cognition efficiency.

The OTM enables the inclusion of emerging machine and deep learning applications to seamlessly be integrated into the orchestrated environment to constantly evolve the cyber security solution to adapt to the changing threat landscape. Some other areas of machine learning that are under research with Wedge Networks' OTM include: the use of Google's Deep Learning for anti-spam purposes; and the use a TensorFlow machine learning algorithm for web filtering purposes – this algorithm allows the automatic classification of a web page based on its attributes such as the pages linked to/from the page.

2.4 Security Orchestration Layer

The Security Orchestration layer is functionally similar to an SDN and network functions virtualization (NFV) orchestrator, however the primary scope is limited to controlling the OTM resources. It is also desirable for the orchestrator to support a limited set of SDN switch functions to automate the provisioning of security in-line with data services and possible remediation of certain security threats.

At a rudimentary level, the Security Orchestrator provides the administration of the OTM platform's software and hardware resources, much like an element management system controls a UTM security appliance. The major difference is that the orchestrator operates on a paradigm of abstraction, where orchestration software is decoupled from intricacies of the lower level hardware and software. The result is the OTM platform is highly programmable and easily customizable to support a wide range of use cases and an expanding set of security applications.

The Security Orchestrator can directly control the hardware or interface with OpenStack or VMware to control the virtualized compute resources. Similarly, it can directly control the applications and coordinate with the Security Mediation layer resources, or manage an independent VNF as part of the OTM ecosystem. Additionally, the Security Orchestrator may control a virtualized Ethernet switch using OpenFlow™ to facilitate the automated mapping of service flows through the OTM platform. This range of control positions the Security Orchestrator to facilitate service chaining of a range of security functions, applying security technologies and applications from multiple vendors, with common operations using a single pane of glass.

2.4.1 Why Use a Dedicated Security Orchestrator?

Some have asked why a separate and dedicated security orchestrator is required, as opposed to using an existing cloud or network orchestrator. The short answer is that in most cases those orchestrators are not present in production networks, and when they are, most will not be focused to efficiently manage the security applications and security mediation functions with the same level of efficiency and granularity. At some point the industry may specify international standards to facilitate that capability, however that process will likely take several years to materialize. In the interim, the concept of SDN and orchestration provides the option for higher level orchestrators to interface with and control lower level application specific orchestrators. So the service orchestrator will have a productive role even as higher level orchestrators are introduced over time.

2.5 Alternative Approaches for Cloud-Layer Security

Many incumbent vendors have begun marketing their existing UTM and NGFW appliances for deployment at the cloud-layer to cover expanding premises-based security gaps. The following sections address the numerous reasons why this approach is undesired and why OTM is a preferred approach.

2.5.1 Physical Appliances: Good for Vendors, Not so Good for Enterprises, Service Providers or Emerging Networks

Much like router and switch vendors, conventional security appliance vendors love to develop and sell hardware appliances. Vendor investments in hardware acceleration technology and proprietary ASIC developments gave early security vendors tangible differentiation that was costly and difficult for competitors to match. Once a customer deployed their solution, it was difficult for another vendor's product to displace the incumbent solution due to operational complexities with a phased transition or upfront displacement costs with a full cutover.

What made this appliance business model even more attractive for vendors was that the model of embedding operating system (OS) and application software in these appliances locked the software in the associated hardware appliance. If the hardware was retired, the software was too. Each appliance was designed to support a specific maximum capacity of traffic, so customers naturally purchased appliances with substantially more capacity than they needed initially to extend the useful life of the asset for a longer depreciation period. The result was that Enterprise customers received no credit for the software they previously paid for when upgrading, and they typically paid for substantially more security capacity than they initially required, upfront. This was a great model for vendors, but not so great for Enterprises or service providers planning to use their appliances.

When you consider the scale and pace at which traffic is growing today, particularly with cloud-based data centers and applications, the projected traffic capacity requirements translate into a need for massively scalable systems which are not well addressed by static, fixed-capacity appliances. Furthermore, the evolving software-

defined nature of networks and the emergence of NFV is creating the opportunity for networks to become dynamically configured, scaling capacity up and down over time, and reconfiguring to support changing connectivity requirements. The fixed capacity and statically managed nature of security appliances is simply not well aligned with rapidly evolving more agile and orchestrated networks. Security platforms must also evolve to embrace cloud-based computing to scale as flexibly and dynamically as the services being protected. The software must become abstracted from the proprietary appliance hardware, and designed to operate on commercial off the shelf (COTS) hardware. And ideally, the software should allow for operation in a SDN and NFV orchestrated environment to achieve the agility, performance and scale of the services and networks being protected.

2.5.2 Virtual Appliances: Necessary, But in Many Case Not Sufficient

The dramatic industry movement toward NFV has started an irreversible trend toward virtualizing legacy appliance products to run as software on top of industry standard server hardware. This trend has put pressure on nearly all equipment vendors to offer VNF instances of their physical appliances, often referred to as virtual appliances. In most cases, conventional security appliance vendors have little history or expertise in working with higher level operational software trends like SDN or NFV orchestration. So it's only natural that most security vendors have simply focused on taking their existing software and adapting it to run on as a virtual machine (VM), and then marketing them as a virtual appliance.

2.5.2.1.1 VNFs Require an Orchestrator, Frequently Not Available

While developing VNFs is an important step in the right direction, in most cases the results to date have been mixed for vendors and their customers alike. The first challenge is that while SDN and NFV orchestrators are evolving rapidly, very few are in operation for anything other than large scale data center cloud compute and storage applications. A handful of SDN and NFV orchestration vendors have taken on the task of integrating high level service chaining support for a variety of software defined network elements and VNF products, however very few of these orchestration systems are in place and ready to support full scale security orchestration today. Consequently, the majority of security VNF deployments have been in proof of concept trials and labs to demonstrate the concept of spinning up virtual appliances as part of a service chained end-to-end service.

2.5.2.1.2 Porting Legacy Software to Run as a VNF is Not Optimal

Another major problem with most of these security VNF initiatives is that taking security appliance software that was originally developed to run on custom hardware with specialized hardware acceleration does not perform well on COTS hardware. Unfortunately, most traditional test houses that benchmark the relative performance of security appliances have not yet developed comparative test methodologies for objective comparative performance data. So customers have typically accepted a marginally performing virtual appliance or purchased another physical appliance.

While VNFs do create a choice, the vast majority of security VNFs represent the same proprietary, single vendor attributes of physical appliance solutions. They typically lack the open, multivendor technology choices that were a driving objective with SDN and NFV.

Given the inherent incumbent vendor benefits of selling over-capacity designed appliances rather than software scaled to support actual demand, it's unlikely that this situation will dramatically change, at least until OTM platforms become recognized as a compelling alternative.

2.5.3 Multi-Tenancy Versus vCPE Optimized

Most security VNF offerings have been optimized for the virtual customer premises equipment (vCPE) model. The driver behind this model is to eliminate truck rolls by deploying traditional premises-based security functions using a VNF that can be downloaded to run on an x86 server in the premises. While this model has its merits, it's once again focused on the traditional paradigm of protecting the premises and does not address the requirement for cloud layer security.

Service providers require a cloud-layer security solution that supports multi-tenancy, so that one cloud-based security platform (physical or virtual) can be used to provide cloud-layer security to hundreds, thousands, tens of thousands and potentially hundreds of thousands of different end customers, each with their own uniquely specified set of security policies. The single customer orientation of today's vCPE security VNFs do not satisfy this requirement. In theory, the service provider could spin up a unique VNF instance for every end customer serviced from the cloud, however the compute and storage overhead associated with creating and managing large numbers of VNF instances at a single data center location is dramatically less efficient than having a single cloud-based security platform with multi-tenancy support.

3 Evolving Management and Analytics for Continuously Improving the OTM

The previous sections strove to illustrate how an OTM platform is an evolution in cyber defense and how it is able to adapt more easily to the changing threat landscape. The OTM provides the advantages of being able to apply multiple security policies efficiently to the content to identify anomalous activities with a high degree of accuracy including zero day threats. But, for the platform to maximize its capability it must also capture and provide usable analytics that can quickly assist those monitoring to recognize the anomalous activities as well as assist in the machine learning of the system to improve its efficiency. Combining data collection, aggregation and Big Data analytics with machine learning provide greater insights on the evolution of threats; this in turn allows the monitors to better adapt the OTM, if needed, to better predict and respond to network security intrusions.

The adapting OTM is able to populate the system with better information (including information from the private sector, the government and academia), and provide cyber situational awareness across monitored entities, with the ability to spot anomalous activities, analyze those activities and rapidly respond. Examples of advanced useable data collection, analytics and presentation which can assist those monitoring include:

- Indexed event reporting: providing searchable inputs from L3 to L7 of sessions and content for advanced analytics;
- Policy-triggered content capture, export, indexing and archiving: providing powerful data capture for forensics and advanced analytics;
- Elastic search document-based distributed database support: providing an elastic full text search database capability for the indexing and archiving of event logs, exported payloads, mirrored traffic, etc.;
- Event timeline reporting: providing time-line visualization of individual events or sets of events for timeframe-based forensics and analytics
- Analysis Visualization: providing intuitive insights into the threat landscape including a source and destination map to aid in analytics.

3.1 WedgeIQ: A Model for Useable Analytics within an OTM

Using Wedge Networks' OTM management tool, WedgeIQ, as a model, the following sections provide detail into the bullets listed above as an example of analytics that can quickly assist those monitoring to recognize the anomalous activities as well as assist in the machine learning of the system to improve its efficiency.

3.1.1 Indexed Event Reporting

WedgeIQ provides searchable inputs from L3 to L7 of sessions and content for advanced analytics through the use of session reconstruction. Within the WedgeOS, data is passed through both DPI and DCI scanners providing full L3 to L7 visibility. The proper management of events from the DCI Engine and DPI Engine is put in place so that these events can be indexed. Session reconstruction works differently for each service type:

1) DPI – With Deep Packet inspection, traffic mirroring (packet mirroring) is setup and is triggered when certain categories are triggered. For example, if traffic mirroring is set up for "Chat", whenever the DPI engine triggers on that rule, it will copy and forward all packets to a server where the session can be reviewed. In one Wedge deployment, the Moloch interface was used to reconstruct the TCP sessions.
2) DCI – With Deep Content Inspection, this reconstruction was developed by Wedge whereby if any DCI policy is triggered, the "payload" that it was triggered on is sent to the Event Archive server where Mail and HTTP session reconstruction takes place.

Once information from DPI and DCI are captured and indexed in ElasticSearch (ES), the WedgeIQ Dashboards / Investigations / Log Drill Downs / Etc. simply read from the ES document database to populate its User Interfaces. Each dashboard / page has the ability to filter or even search on any content that has been displayed.

3.1.2 Policy-Triggered Content Capture, Export, Indexing and Archiving

File attachments and emails that are exported from WedgeOS and WedgeOS instances in Wedge Cloud Network Defense are indexed and archived. This provides powerful data capture for forensics and advanced analytics. This relies on the DPI and DCI Indexed Event Reporting described earlier, with DPI using traffic mirroring and DCI using event exporting, to get the data to the ElasticSearch function. The data is then populated in the User Interfaces. The key with WedgeIQ is that it only exports data when a policy is triggered and when the system has the "export flag" set to "on"; so the system knows to export the payload. If exporting is turned "off", the payload is removed from WedgeOS after it is scanned and delivered to its destination (the client or server).

3.1.3 Elastic Search Document-Based Distributed Database Support

This feature of WedgeIQ provides an elastic and full text search database capability for the indexing and archiving of event logs, exported payloads, mirrored traffic, etc. A full text search database ElasticSearch technology is chosen for the index and archive of the event logs, exported payloads, and mirrored traffic from WedgeOS, Web Application Firewall (WAF), and Wedge Cloud Network Defense. The ElasticSearch solution provides an expandable cluster-based solution that can grow in computational and archiving capability. It also provides a simple REST API to retrieve data for visualization or external analysis. ElasticSearch is used on the back-end of WedgeIQ to store all of these events as "JSON documents". Once the data is in, users can search and filter based on the content. Searching by IP address (or client), Tenant, DCI categories that were triggered, etc. are all possible.

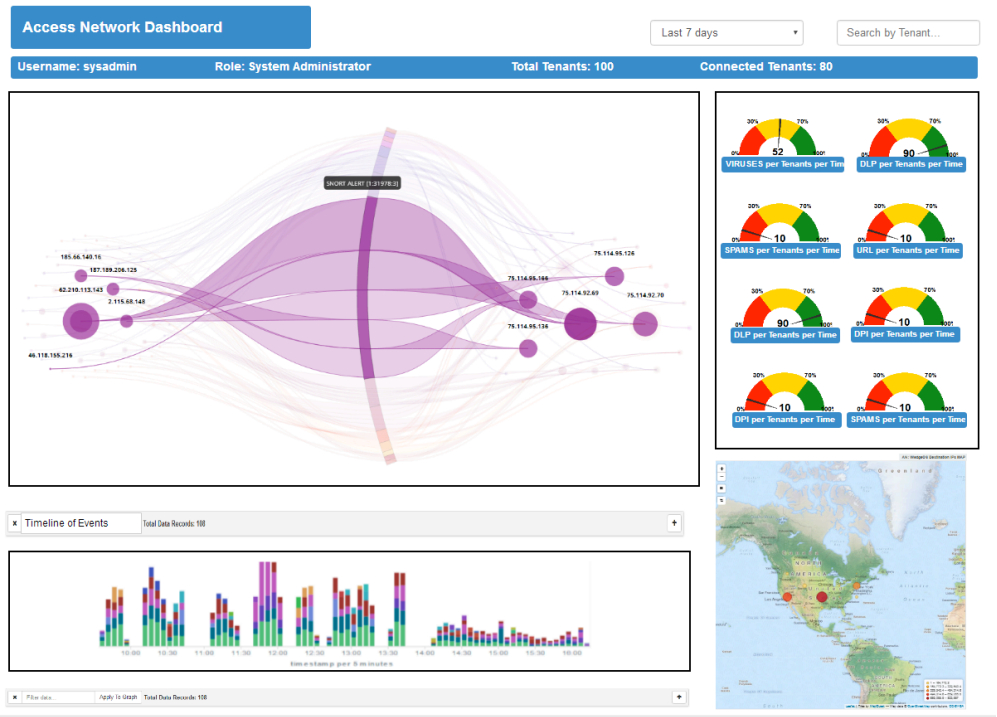

Figure 5) Sample Data Center Dashboard

3.1.4 Event Timeline Reporting

Event Timeline Reporting provides time-line visualization of individual events or sets of events for timeframe-based forensics and analytics. The WedgeIQ Event Timeline is an analysis visualization that allows for a timeline-based analysis of when events are occurring. The types of events that provide the timeline lanes of the visualization is selectable by the user,

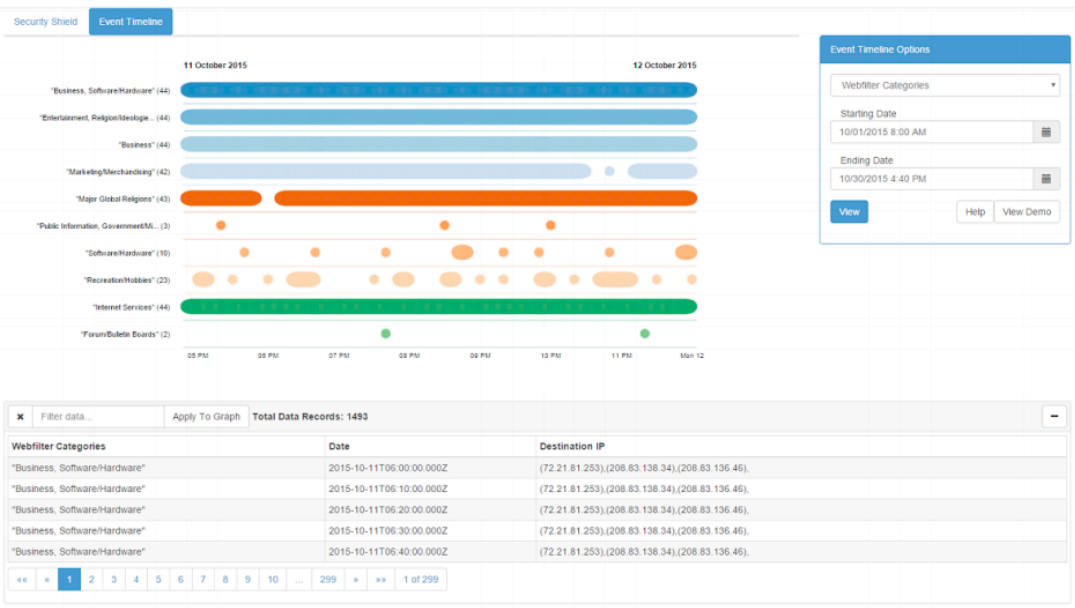

Figure 6) Sample Event Timeline

along with the timeframe of interest. Individual events can be isolated and details can be made visible. The events can be filtered further to provide a focused timeline view. This is one of the dashboards that is provided in WedgeIQ along with the Security Shield. It allows visualization of "time" components to provide information on when an event or series of events occurred on the network. It is grouped by category on the Y-axis so that events can be grouped by the type or category that they belong to. For example, a user could see all WebFilter categories that were triggered, along with when they were triggered.

3.1.5 Analysis Visualization

The WedgeIQ Security Shield is an analysis visualization that allows for intuitive analysis of security events that are most commonly triggered and the source or destination endpoints involved. The types of events that define the visualization can be selected by the user along with the timeframe of interest. The visualization can be filtered further. The endpoints or the selected parameter in the visualization can also be highlighted so that relationships can be viewed. This is one of the dashboards that is provided in WedgeIQ along with the Event Timeline described earlier. It is a visualization that has a "shield" superimposed on the events that were triggered. This allows users to identify where the attack came from (the source address) along with what is being attacked (the destination address). This visualization helps to quickly identify what types of attacks are occurring, as well as if an attack is against a single server or against multiple servers.

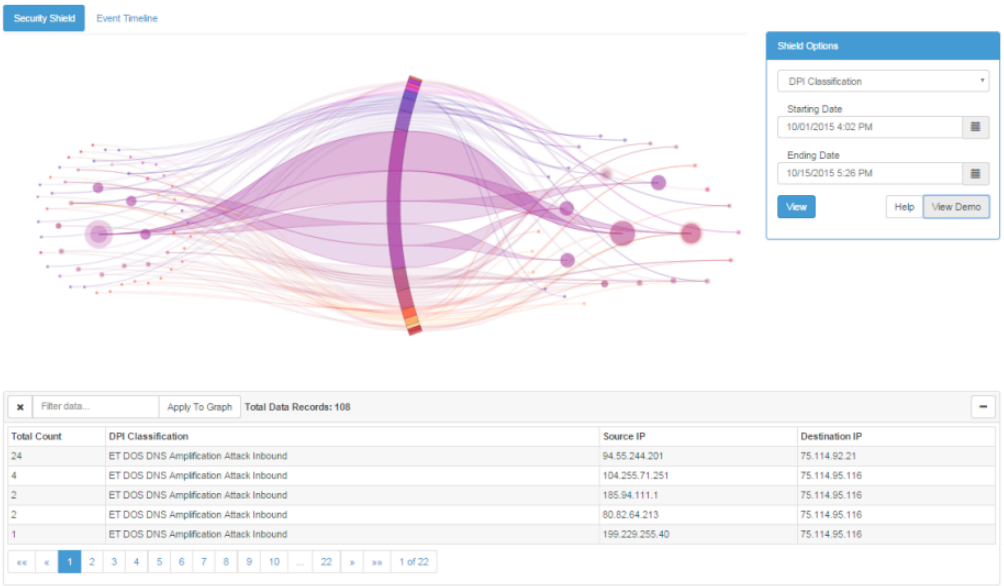

Figure 7) Sample of WedgeIQ Security Shield

3.2 Real-Time Protection of Networks

For adequate Real-Time protection of networks, security decisions must be made within milliseconds, before packets are dropped. Thus, in order for cyber defense to be effective, it needs to offer: 1) L3-L7 Data Discovery, 2) Both pattern matching and artificial intelligence analysis (as compared to threat intelligence), and 3) Decision making, or a course of action, within this milliseconds window. In addition, an effective solution should provide actionable feedback for quick identification of threats, as well as provide a learning environment to improve on the three items mentioned.

WedgeIQ provides Real-Time protection through Wedge Cloud Network Defense, which uses a combination of its WedgeOS platform, multiple security NFVs, and WedgeIQ analytics and policy enforcement. WedgeIQ is the data science based service that provides Big Data functionality, employing unique threat detection and remediation algorithms, along with a variety of pattern-matching and machine learning techniques to identify

targeted cyber threats against end-users. It enables real-time response to security outbreaks and presents the results in a variety of easy to understand analytics.

Each of the various WedgeOS instances deployed globally are continually collecting and processing network data in real-time with no queuing. WedgeOS has full visibility of Layer 3-7 data content and scans all traffic, providing the Deep Data Discovery, pattern matching and artificial intelligence analysis, and ultimately the decision making or course of action; all in real-time with no perceptible latency. Intelligence on the data is communicated back to WedgeIQ, which offers more detailed analytics and continuously updates the new intelligence, along with any updated policy enforcement, back to each of the WedgeOS instances. WedgeIQ also monitors the health of the WedgeOS instances and ensures that each instance is updated with all of the latest intelligence from security partners as well as its own artificial intelligence analytics. This feedback loop of real-time scanning, analysis, decision-making and policy enforcement between WedgeOS and WedgeIQ, along with the provision of usable analytics that can quickly assist those monitoring to recognize anomalous activities, are what enables an effective network cyber defense.

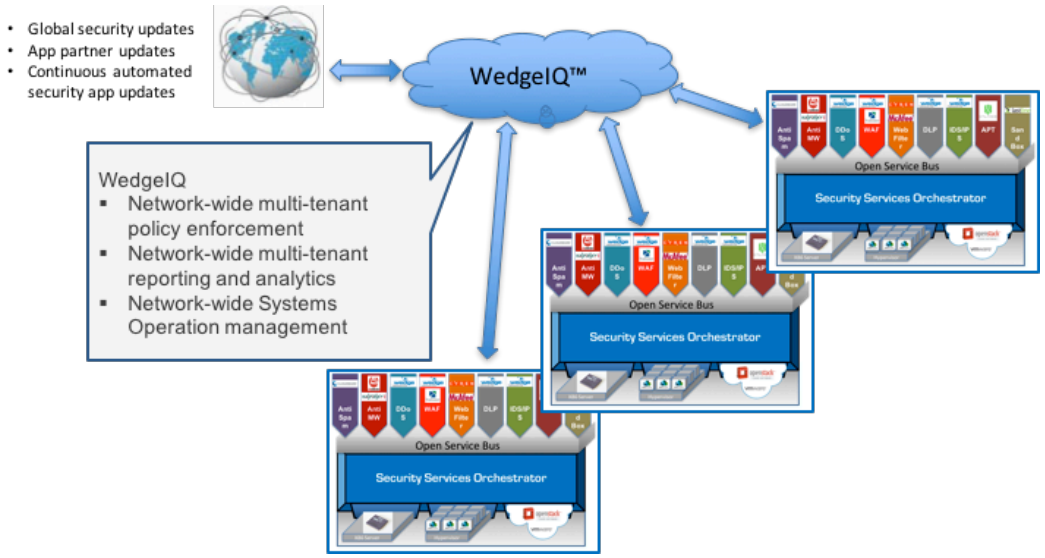

Figure 8) Real-Time Protection with WedgeIQ

4 Concluding the Case for OTM

Orchestrated Threat Management represents the next logical step in the implementation of security functions. It represents an opportunity to overcome many of the undesirable constraints of dedicated proprietary UTM and NGFW appliances of the past, and incorporate the new capabilities and attributes of rapidly evolving software-defined, programmable networks that promise to revolutionize the communications industry.

While OTM platforms can be deployed in any environment, the maximum benefits of OTM are achieved when deployed in a cloud computing environment. Most of today's government, leading enterprises and service providers have invested heavily in establishing their own scalable cloud computing environments, so adding OTM as a security application is a logical use of that resource and an ideal way to establish a massively scalable cloud-layer of security.

By deploying OTM at the cloud layer, government, enterprises and service providers can begin to offload security functions from premises-based appliances, allowing those devices to remain in place and support a subset of security applications that are well within the scope of their hardware constraints. This provides the perfect combination of closing critical security gaps, providing a cap-and-grow strategy for the incumbent

security systems, and position for the massively scaling, more dynamic requirements of emerging networks and business.

As the industry's first OTM platform, Wedge Networks' Cloud Network Defense with WedgeIQ provide example of capabilities an OTM can provide as well as the variety of reporting, archiving and analytical tools that could improve cyber situational awareness across government agencies and the ability to detect and respond much more rapidly to threats than it is currently able to. Wedge Networks Cloud Network Defense provides real-time ability to capture data in motion with full visibility of Layer 3-7 data content, and is able to apply multiple security policies efficiently to the content with no latency induced reprocessing to identify anomalous activities with the highest degree of accuracy including zero day threats. Furthermore, WedgeIQ captures and provides improved visual analytics that can quickly assist those monitoring to recognize the anomalous activities. In addition, WedgeIQ assists in the machine learning of the system to improve efficiency.