ARBOR NETWORKS
The Security Division of NETSCOUT

White Paper

NEXT GENERATION DDoS SERVICES

Broader Reach, Faster Delivery, Reduced Cost, and Increased Revenue with NFV

About Arbor Networks

Arbor Networks, the security division of NETSCOUT, is driven to protect the infrastructure and ecosystem of the internet. It is the principle upon which we were founded in 2000; and remains the common thread that runs through all that we do today. Arbor's approach is rooted in the study of network traffic. Arbor's suite of visibility, DDoS protection and advanced threat solutions provide customers with a micro view of their network enhanced by a macro view of global internet traffic and emerging threats through our ATLAS infrastructure. Sourced from more than 400 service provider customers, ATLAS delivers intelligence based on insight into approximately 1/3 of global internet traffic. Supported by Arbor's Security Engineering & Response Team (ASERT), smart workflows and rich user context, Arbor's network insights help customers see, understand and solve the most complex and consequential security challenges facing their organizations.

To learn more about Arbor products and services, please visit our website at arbornetworks.com.

Introduction

Technology adoption in the enterprise is driven by business need. Over the past few years a wide range of small, medium and large enterprises representing every market vertical have rapidly moved to the cloud, embraced SaaS, exploited mobility and become ever more dependent on the connected world. There is no doubt these new technologies have enabled new business models – but they have also created new security risks and increased exposure to cyber-attacks such as Distributed Denial of Service (DDoS).

DDoS, in particular, has gone through a step change over the last 18-24 months. The size, complexity and frequency of attacks have increased dramatically due to the weaponization of DDoS botnets. The attacks in late 2016 on DYN's managed DNS infrastructure is a cautionary example of the damage that can be done. Businesses are becoming more broadly aware of the risks they face from DDoS and are looking for services and solutions to mitigate these risks.

ISPs and Managed Security Service Providers (MSSPs) are ideally placed to address these needs: they have experience offering managed security services to their larger customers and are always looking for ways to maximize the revenue they can generate from their network infrastructure and skilled employees. Until recently, ISPs and MSSPs faced considerable challenges scaling managed security services to the small and medium-sized enterprise markets. Now, however, it is possible to package and deliver these services to a much broader range of organizations thanks to Network Function Virtualization (NFV) and maturing service management and network orchestration systems (MANO). Using these innovations, ISPs and MSSPs can finally achieve the necessary agility to deliver automated, streamlined service provisioning and operational controls.

Smarter Attackers, Smarter Attacks

A combination of factors has led to a dramatic increase in the complexity, frequency and impact of DDoS attacks.

COMPLEXITY

Multi-vector attack combines high volume, application and state exhaustion attacks against infrastructure devices all in a single, sustained attack.

48%
of Enterprises

20%
Increase

Source: Arbor's Worldwide Infrastructure Security Report

FREQUENCY

Driven by inexpensive for-hire attack services and free attack tools.

7.5 MILLION
DDoS attacks

20,604
Attacks per day

Source: Arbor's ATLAS Infrastructure

IMPACT

Big increase in overall business impact from DDoS attack.

57%
Reported reputation/ brand damage

12%
See costs of over $100K, 5x the proportion in 2016

Source: Arbor's Worldwide Infrastructure Security Report

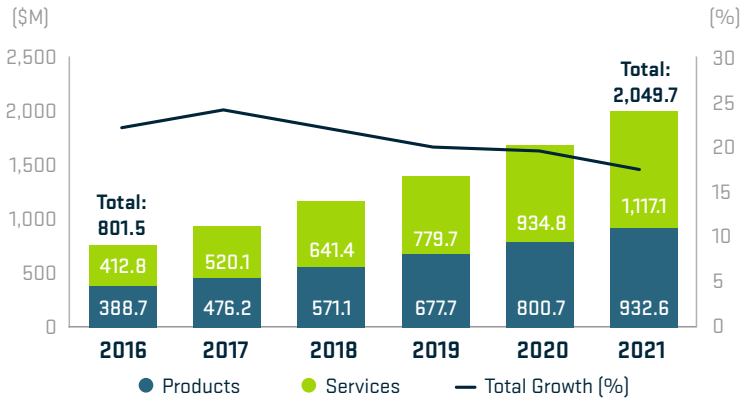
Next-Generation Services

From virtual firewalls to email security, from vulnerability scanning to DDoS attack protection, the market for security services is growing steadily (Figure 1).

In order to deploy and deliver these services more pervasively improvements are needed: the provisioning process must be simplified; they must become more automatic and API-friendly to minimize operational integration and overhead; and they must be cost-effective in a world shifting towards on-demand and elastic consumption. To address these automation, integration and operational challenges service providers are turning to NFV.

NFV is now emerging from the hype stage and entering mainstream adoption. The promise of running applications as virtual network functions (VNFs) on demand makes networks more open, scalable, predictable and flexible, which leads to reduced operational costs and increased user satisfaction. However, NFV is not just an evolution in networking technology, it reflects significant changes to service providers' operational assumptions and business models as traditional architectures and modes of operation come under increasing strain from evolving market demands.

Worldwide DDoS Prevention Products and Services Revenue Overview: 2016-2021 Revenue ($M) with Growth (%)



Source: IDC, 2017

Figure 1: DDoS service growth

This document provides the MSSP or ISP with Arbor Networks' vision and strategy for how to successfully deliver the next generation of NFV-driven DDoS managed services.

Arbor's NFV strategy is focused in the three areas:

1. Virtualizing platforms and services
2. Introducing flexible licensing to support elastic business models
3. Enabling operators to integrate Arbor's solutions into any orchestration environment

How NFV Enables Faster Service Rollout

NFV is a step toward function-defined workflows and dynamic associations of hosted services, and enables a more fluid service-provisioning model. NFV is already spurring numerous carrier, cloud, hosting provider and large enterprise deployments at scale for these reasons.

Fixed and mobile network operators are leveraging Software Defined Networking (SDN) and NFV to offer dynamic service orchestration of virtualized firewall, IDS, NAT, SD-WAN, WAN acceleration and other virtualized network functions (VNFs), while SDN takes care of service chaining VNFs and forwarding traffic to and from the customer.

Service providers have turned to SDN to provision overlay services on top of their existing network infrastructure, leveraging the benefits of SDN (including centralized control, rapid and automated provisioning, hardware independence) without incurring the costs of replacing legacy equipment. VNFs can run in a service provider datacenter, often called "telco cloud" or "virtual CPE", or directly on CPE appliances, which are sometimes called NG-CPEs for their ability to host 3rd party applications in the form of VNFs.

When it comes to telco cloud deployments, the service provider industry has pretty much consolidated on the architecture proposed by the European Telecommunications Standards Institute (ETSI) (Figure 2). In this architecture, the service provider utilizes a MANO that deploys, maintains and terminates VNFs as well as the connectivity among them. VNFs are 'on-boarded' in the MANO when an operator wants to roll out a new service or new application.

In many cases, service providers are offering (or looking to offer) a service portal where customers can self-select and automatically invoke the services they need. The service portal notifies the MANO and OSS/BSS systems to deliver the necessary capabilities. The MANO deploys the VNFs responsible for implementing the service. Services might be as simple as standalone virtual firewalls and virtual anti-DDoS appliances, or as sophisticated as a service chain that enables traffic flow across several VNFs before reaching the customer. The MANO also interfaces with the OSS/BSS for billing purposes.

MSSP customers can subscribe to security services on the portal and have the services provisioned and activated within minutes without any need for physical infrastructure changes within their network or the service provider's. The result is an easy, 'on-demand' way for customers to access the services they need to mitigate their business risk — delivered more quickly and cost-effectively than was previously possible.

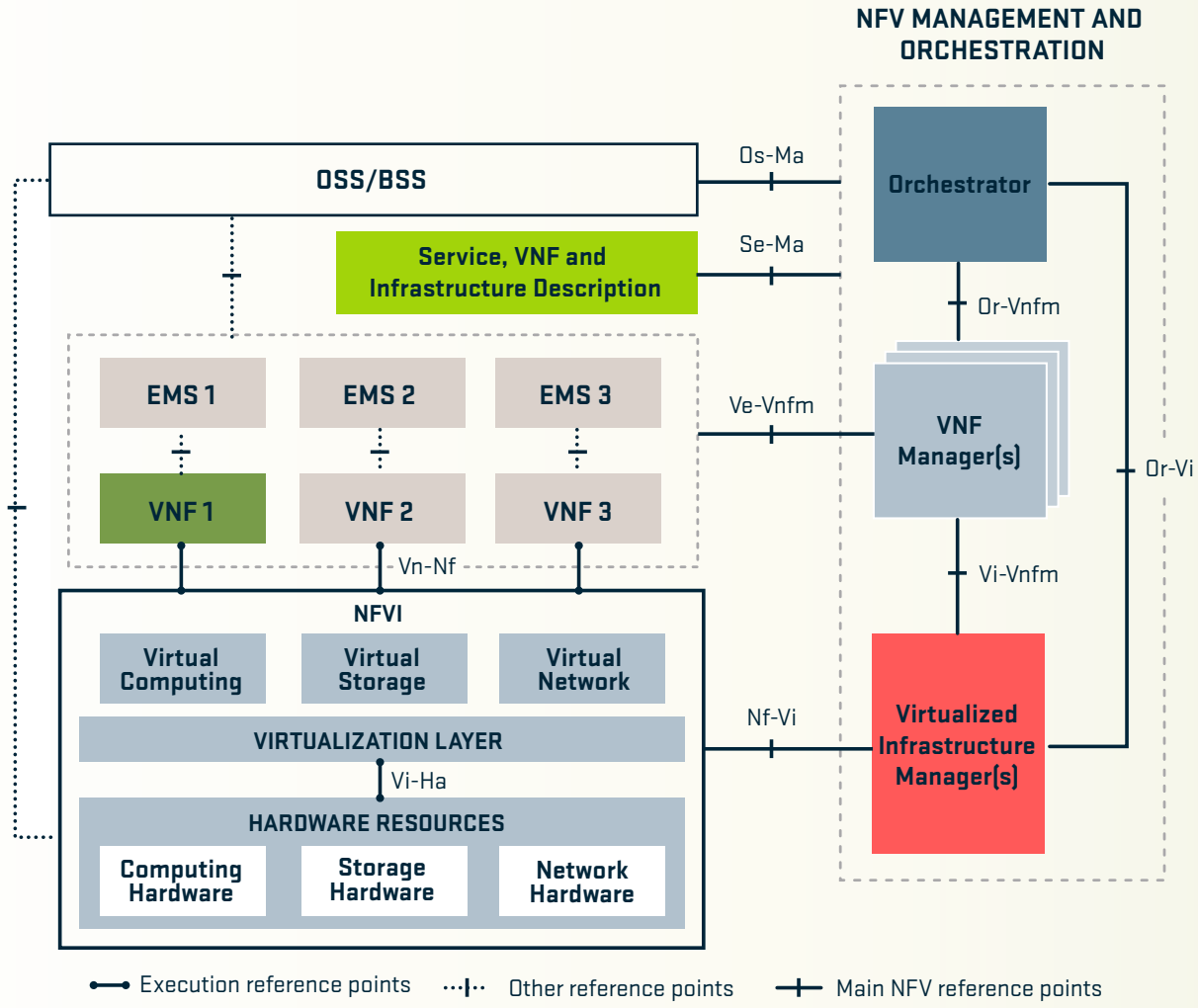


Figure 2: ETSI NFV architecture

These new network capabilities allow service providers to deliver services to a much broader range of customers, at much higher scale and lower cost – maximizing service profitability and increasing stickiness.

Arbor is convinced this model will see broad adoption within the ISP/MSSP market and is actively working to support this effort within its customer base.

ARBOR: WORKING WITH NFV TODAY

Virtualization & Automation

Arbor Networks has fully virtualized its Network Visibility and DDoS protection platforms to provide customers the flexibility they need to fit any network architecture and protection model.

Many Arbor ISP/MSSP customers have already deployed virtual Arbor SP so they can use their own hardware and infrastructure, but these deployments are not usually provisioned dynamically using a MANO system. Arbor SP is used to monitor network routing infrastructure, and thus the scale of deployment is not directly driven by customer service demand. Similarly, Arbor's TMS solution is designed to be deployed within ISP/MSSP networks as a physical appliance, as a VM or on bare-metal to provide high volume DDoS mitigation capability, and thus dedicated bandwidth is usually provisioned. This dedicated bandwidth prevents other services being impacted during a DDoS attack when traffic is diverted to the TMS infrastructure for cleaning.

When it comes to enterprise/cloud DDoS protection strategies, security experts increasingly recommend a layered or hybrid approach combining on-premises and cloud-based mitigation capabilities for maximum effectiveness. This gives the organization a scalable defense solution that can adapt to different types and sizes of attacks. Arbor offers a comprehensive portfolio of virtual and appliance-based solutions supporting this hybrid approach (Figure 3).

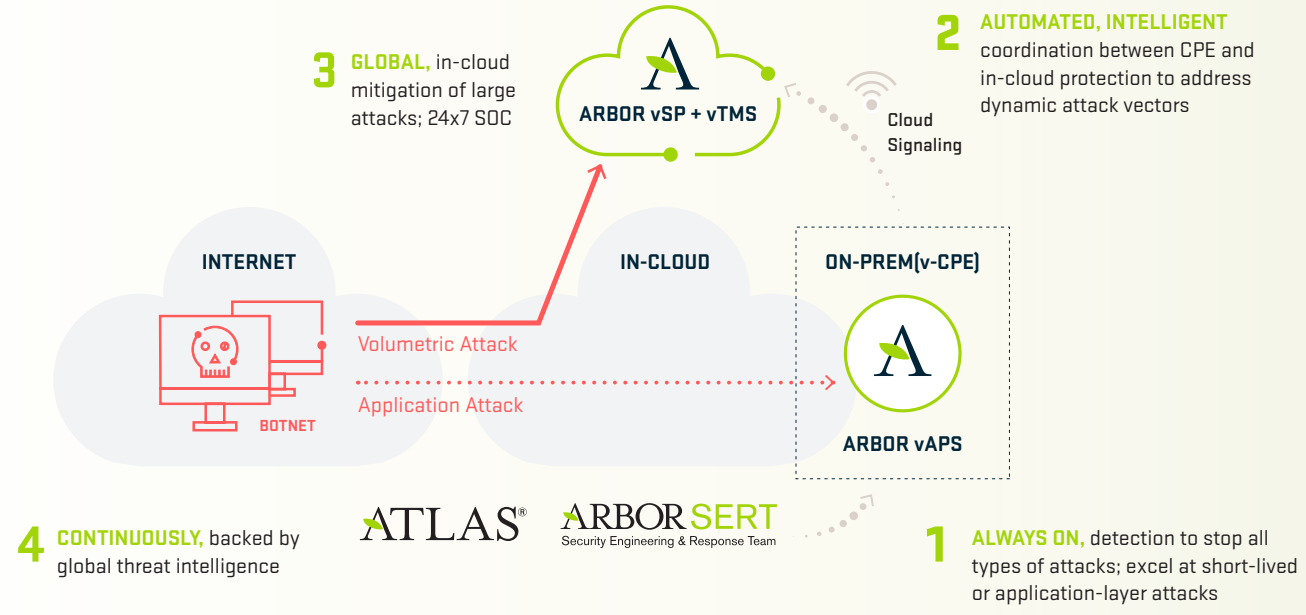


Figure 3: Virtualized and multi-layered DDoS protection

The full value of the multi-layer defense model, with Arbor vAPS in a key supporting role, includes:

Immediate attack response

Thanks to vAPS' inline, always-on deployment.

Application-layer detection and real-time protection

vAPS is directly inspecting packets and in the path of traffic.

Segmentation of responsibility

Different groups can manage the in-cloud volumetric protection vs. the always-on, customer-specific vAPS instance (either a separate service arm of the managed service provider, or even the enterprise customer themselves).

Segmentation of privacy

Important policy, such as SSL decryption private keys and certificates, can be managed separately on the APS by the end customer, removing the service provider from having to manage that sensitive and proprietary information.

Visibility

Last but definitely not least, never underestimate the power of visibility this kind of always-on service can provide — regarding security (observed threats, data about attacks, etc.) but also about general service activity and business questions such as what geographic markets are accessing a service, and what is the historical and current trend of traffic volume for different services. Top URLs, top FQDNs, and other application-layer data can provide a lot of operational value to groups that may not have the tools to glean this data or may not have access to tools that exist in other parts of the organization.

Arbor vAPS is designed from the ground up with the enterprise in mind, and has a simple easy-to-use user interface. Once configured, the APS can automatically mitigate most DDoS attacks, and provides a wealth of additional forensic reporting. APS can also automatically block in-bound/out-bound traffic to/from known bad actor infrastructure on the Internet, using Arbor's ATLAS Intelligence Feed (AIF).

ATLAS is a collaborative project with 400+ customers who share 140+ Tbps of anonymous traffic data.

With this unique network lens, we study threat actors, their tools, behaviors and campaigns on a global basis. Arbor customers enjoy a considerable competitive advantage: a micro view of their network combined with a macro view of global Internet traffic. This powerful combination of network security intelligence is unrivalled in the market

ARBOR: WORKING WITH NFV TODAY

Flexible Licensing

In order to support a range of virtualized environments, all Arbor DDoS products can be installed on top of major open-source and commercial hypervisors and are offered under flexible licensing models.

Arbor licensing is based on "capacity pools" that allow operators to dynamically enable protection capacity (in the form of vAPS instances) wherever and whenever they want. For example, an MSSP could license a 10G pool and offer a 1Gbps managed service to ten different customers, 100x 100Mbps or any mix of supported throughputs. And, licenses can be moved from customer to customer, scaled up or down and even re-used as customers join the service, as their capacity needs change or as they leave the service.

This virtual site license capacity can be purchased either as a perpetual license or as a month-to-month subscription, making vAPS a good fit for any business model and ideal for MSSP service rollouts, since the network operator is only obligated to pay as they grow.

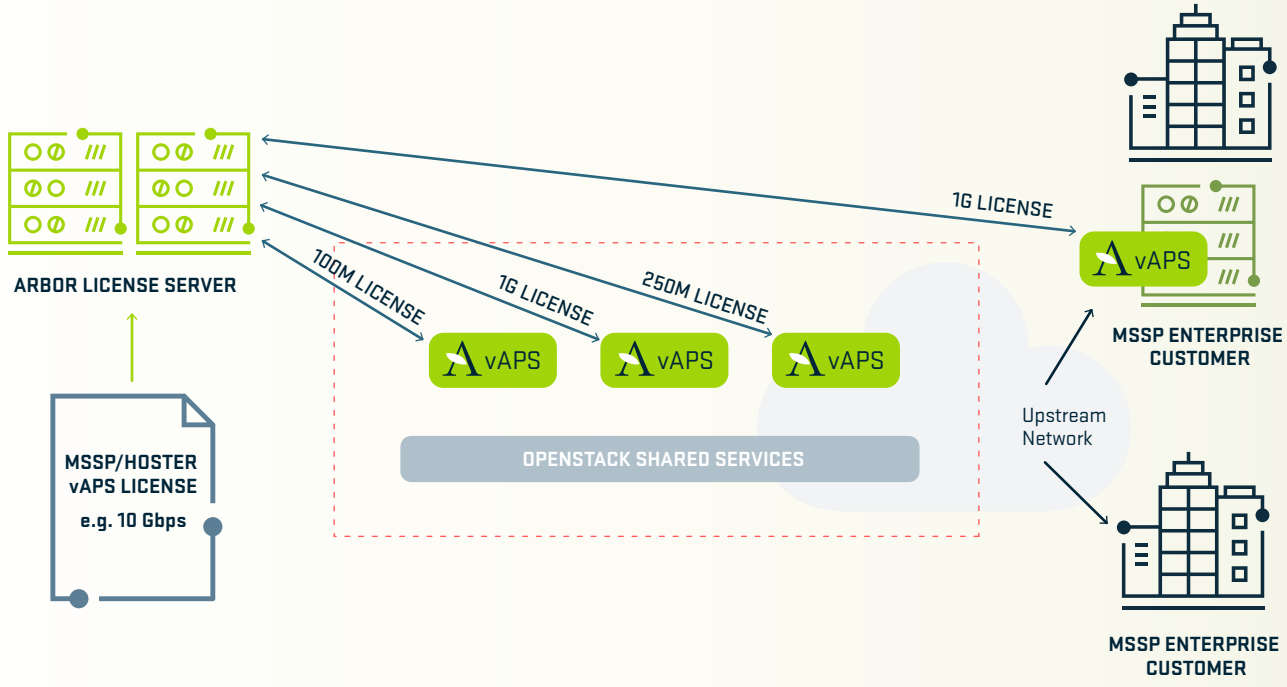


Figure 4: Arbor virtual site license capacity pools model

ARBOR: WORKING WITH NFV TODAY

MANO Integration

Arbor already has considerable experience deploying our DDoS solutions in vendor-neutral virtualized environments. In order for DDoS protection services utilizing a vAPS VNF to be provisioned by a MANO system, several components are required:

Service descriptors for the infrastructure requirements and capabilities of the VNF.

These descriptors take the form of templates, often formatted as TOSCA, YAML or XML, depending on the environment. Example templates are available from Arbor today. Arbor has already developed templates for use with Cisco NSO/ESC, OpenStack Tacker and Nokia CloudBand.

The VNF must be configurable.

Arbor vAPS supports integration with Cloud-init and OpenStack to automatically create and configure vAPS instances. All Arbor products, including vAPS, have a full REST API to enable ongoing configuration

VNF monitoring and life-cycle management.

The health of vAPS instances must be monitored, so that failures can be detected via log data or REST API, and appropriate healing operations can be triggered (e.g. service re-deployment and underutilized vAPS instances can be terminated and revived on demand.) Arbor vAPS supports integration with Heat, Tacker, and Ansible for VNF management.

Arbor has already successfully on-boarded vAPS into a number of MANO platforms, including both market leading commercial orchestrators (Cisco NSO, Nokia CloudBand) and open-source platforms like OpenStack Tacker.

ARBOR: WORKING WITH NFV TODAY

The Future

Arbor is fully committed to enabling its ISP and MSSP customers to maximize their business opportunity from DDoS Protection services. Arbor is looking at a number of key areas for future development around NFV MANO:

- vAPS onboarding support for a wider range of MANO ecosystems.
- Additional life-cycle management monitoring and scaling functionality for vAPS.
- Additional element management capabilities via a multi-tenant vAPS console.
- Integration of vAPS with NG CPE platforms from a number of leading vendors.
- Additional automation of vAPS configuration and tuning processes to support fully hands-off deployment.

CONCLUSION

As more enterprises become more dependent on the connected world, and become more aware of the risks they face, they are looking for best-of-breed defenses. However, unlike large enterprise, many small and medium enterprises lack the resources to operationalize defensive technologies – they need managed services.

ISP and MSSPs are well positioned to deliver these capabilities, but they must be able to do so using an operational model that gives them the agility and cost-base that they need. NFV MANO addresses these needs, and vAPS from Arbor can provide the core component of a managed hybrid DDoS defense service.

By combining Arbor's market leading DDoS defense technology with NFV MANO, ISPs and MSSPs can offer their customers the ability to consume the technologies and services they need when they need them, with minimal operational overhead or upfront commitment on either side.

Learn More

For further information please contact you Arbor account team.

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales
Toll Free +1 855 773 9200

Europe
T +44 207 127 8147

Asia Pacific
T +65 6664 3140

Latin & Central America
T +52 55 4624 4842

www.arbornetworks.com

ARBOR® NETWORKS

The Security Division of NETSCOUT

WP/NEXTGENERATIONDDoS/EN/0218-LETTER