

The 2014 Application & Service Delivery Handbook

Executive Summary

By *Dr. Jim Metzler, Ashton Metzler & Associates
Distinguished Research Fellow and Co-Founder
Webtorials Analyst Division*

Platinum Sponsors:



Gold Sponsors:



Produced by:



Executive Summary

Introduction	1
Second Generation Application and Service Delivery Challenges	2
Mobility and BYOD	2
Virtualization	2
Cloud Computing	3
Software Defined Networking	4
Network Function Virtualization	4
Network and Application Optimization	5
Key Optimization Tasks	5
WAN Optimization Controllers (WOCs)	5
Application Delivery Controllers (ADCs)	5
NFV Optimization	7
Emerging WAN Optimization Services	8
Emerging Environment	8
Cloud-Based, Private WAN Optimization Solutions	8
The Optimization of Internet Traffic	8
Hybrid WAN Optimization Solutions	8
Management	10
Key Management Tasks	10
Impact of SDN	10
Application Performance Management	11
A Framework	11
Application Aware Network Performance Management	11
DevOps	12
Security	13
The Changing Security Landscape	13
Current State of DDoS Attacks	13
Web Application Firewall Services	14
Impact of SDN	14

Introduction

Throughout the **2014 Application and Service Delivery Handbook** (*The Handbook*), the phrase **ensuring acceptable application and service delivery** will refer to ensuring that the applications and services that an enterprise uses:

- Can be effectively managed;
- Exhibit acceptable performance;
- Incorporate appropriate levels of security;
- Are cost effective.

There is a growing relationship between the requirements listed above. For example, in order to implement an appropriate level of security, an IT organization may implement encryption. However, the fact that the information flow is encrypted may preclude the IT organization from implementing the optimization techniques that are required to ensure acceptable performance.

Starting around 2007, IT organizations began to implement the first generation of application delivery solutions in order to respond to the first generation of application delivery challenges, such as supporting chatty protocols. The first generation of application delivery solutions were typically deployed on-premise. Representative solutions included appliance-based WAN Optimization Controllers (WOCs), management solutions that focused narrowly on the network and myriad security appliances such as firewalls.

A second generation of challenges is described below. To respond to these new challenges a second generation of application delivery solutions is emerging. In many cases these solutions aren't appliance based, but are software based. In a growing number of instances they are provided as part of a managed service or acquired from a public cloud provider. The management component of this new generation of application delivery solutions is less likely to be focused narrowly just on the network and more likely to integrate network and application management.

The goal of the *The Handbook* is to help IT organizations ensure acceptable application and service delivery when faced with both the first generation, as well as the emerging second generation of application and service delivery challenges. To help to achieve this goal, in early 2014 a survey was given to the subscribers of Webtorials. Throughout this document, the IT professionals who responded to the surveys will be referred to as The Survey Respondents.

Second Generation Application and Service Delivery Challenges

There are a number of fairly well understood challenges that have over the years complicated the task of ensuring acceptable application and service delivery. Those challenges are described in detail in the document entitled [Traditional Application & Service Delivery Challenges](#). In addition, there are a number of second-generation challenges that are beginning to complicate the task of ensuring acceptable application and service delivery. Those challenges include:

- Mobility and BYOD
- Virtualization
- Cloud Computing

Mobility and BYOD

Previous research has identified a number of key characteristics that are associated with mobility and BYOD including:

- The vast majority of employees require mobile access for at least part of their typical day.
- The BYOD movement has resulted in a loss of control and policy enforcement.

The Survey Respondents were asked how important it is for their IT organization over the next year to get better at improving the performance of applications used by mobile workers. They were also asked how important it is for their IT organization over the next year to get better at managing and monitoring the performance of applications used by mobile workers. Their responses are shown in **Table 1**.

Table 1: Importance of Getting Better Delivering Mobile Applications		
	Improving the Performance	Managing and Monitoring
Extremely Important	22%	22%
Very Important	33%	33%
Moderately Important	29%	26%
Slightly Important	11%	15%
Not at all Important	6%	5%

Virtualization

Server & Desktop Virtualization

The vast majority of organizations have made at least some deployment of server virtualization and the deployment of server virtualization will increase over the next several years. Many of the same management tasks that must be performed in the traditional server environment need to be both extended into the virtualized environment and also integrated with the existing workflow and management processes. One example of this is that IT organizations must be able to automatically discover both the physical and the virtual environment and have an integrated view of both environments. This view of the virtual and physical server resources must stay current as VMs move from one host to another. The view must also be able to indicate the resources that are impacted in the case of fault or performance issues. Feedback from The Survey Respondents indicates that almost two

thirds of the IT organizations consider it to be either very or extremely important over the next year for them to get better performing management tasks such as troubleshooting on a per-VM basis.

Over the last couple of years desktop virtualization has begun to gain traction in the market. The growing adoption of desktop virtualization is reflected in the fact that well over half of The Survey Respondents indicated that getting better at optimizing the performance of virtualized desktops is either extremely or very important to their IT organization. That is a significant increase over the responses to the same question in 2013 and the responses in 2013 were a significant increase over the responses to that question in 2012.

Software Defined Data Center (SDDC)

As noted, IT organizations are making increasing use of varying forms of virtualization. SDDC is an emerging concept that is being advocated by a number of vendors. The two primary characteristics of a SDDC are virtualization and automation. In particular, in a SDDC, all of the infrastructure is virtualized and delivered as a service and the control of this datacenter is entirely automated by software. The document entitled [*The Promise and the Reality of a Software Defined Data Center*](#) contains a detailed discussion of SDDCs.

Cloud Computing

Both private and public cloud computing create significant challenges relative to ensuring acceptable application delivery. For example, in most instances the SLAs that are associated with public cloud computing services such as Amazon's Simple Storage System are weak and as such, it is reasonable to say that these services are delivered on a best effort basis.

In order to understand some of the concerns that IT organizations have with cloud computing, The Survey respondents were asked to indicate how important it was over the next year for their organization to get better at managing end-to-end in a private cloud environment. **Table 2** shows how The Survey Respondents answered this question in 2014 and also shows how a corresponding set of survey respondents answered this question in 2013.

Table 2: Importance of Getting Better at Managing Private Cloud: 2014 vs. 2013		
	Managing Private Cloud 2014	Managing Private Cloud 2013
Extremely Important	21%	12%
Very Important	39%	30%
Moderately Important	28%	32%
Slightly Important	6%	14%
Not at all Important	6%	12%

Software Defined Networking

According to the [Open Networking Foundation \(ONF\)](#), “Software-Defined Networking (SDN) is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. The OpenFlow™ protocol is a foundational element for building SDN solutions.”

A detailed discussion of Software Defined Networking (SDN) can be found in [The 2013 Guide to Network Virtualization and SDN](#).

Network Function Virtualization

NFV is being driven primarily by telecommunications service providers who feel that they can greatly simplify their operations and reduce expense if all network functions were available as virtual appliances that can be easily provisioned and integrated regardless of the vendor who provided the appliance or the hypervisor(s) on which it runs. In order to bring this vision to fruition, an Industry Specifications Group for Network Functions Virtualization (NFV ISG) was formed under the auspices of the European Telecommunications Standards Institute (ETSI). In October 2013, ETSI published a set of high level reference documents that are openly available on the [ETSI website](#). One of those documents discussed a framework for conducting a NFV Proof of Concept (POC). ETSI currently has eighteen POCs underway.

Until recently, the conventional wisdom in the IT industry was that SDN and NFV were separate topics and didn't need to be formally coordinated. That conventional wisdom changed in March 2014 when the ONF and ETSI announced the signing of a Memorandum of Understanding (MOU) detailing their intention to work together.

A detailed description of Network Function Virtualization (NFV) can be found at [An NFV Reality Check](#).

Network and Application Optimization

Key Optimization Tasks

The Survey Respondents were asked about the importance of a range of optimization tasks. Their feedback indicates that:

- Optimizing the performance of a key set of applications that are critical to the business is the most important optimization task facing IT organizations; followed closely by the need to ensure acceptable performance for VoIP traffic.
- A relatively new challenge, ensuring the performance of applications used by mobile workers, is now one of the most important optimization tasks facing IT organizations.

WAN Optimization Controllers (WOCs)

When WOCs were first introduced in the mid-2000s, they were hardware-based appliances. While that is still an option, in the current environment it is also possible for IT organizations to acquire WOC functionality from a managed service provider (MSP). IT organizations also have a third option because some providers offer network and application optimization as part of a WAN service.

In addition, while it is still possible to acquire a hardware-based WOC, software based WOCs are now available in a number of form factors, including:

- Standalone Hardware/Software Appliances
- Client software
- Integrated Hardware/Software Appliances

Feedback from The Survey Respondents indicates that while there is interest in expanding the use of hardware-based optimization solutions, the primary interest is in expanding the use of software-based optimization solutions.

Application Delivery Controllers (ADCs)

Background

ADCs provide load balancing across local servers or among geographically dispersed data centers based on Layer 4 through Layer 7 intelligence. ADCs also provide a wide range of other sophisticated functionality.

ADCs and Security

The majority of serious security attacks are to an organization's data center because that's where most of their applications and most of their data resides. Given that the most common deployment of ADCs has them placed in front of application servers in a data center, ADCs are in a strategic position to thwart attacks. In order to be effective thwarting security attacks, ADCs should have an ICSA-certified web application firewall, a DNS application firewall and it should also support SSL offload.

IPv6 and ADCs

Some of the IPv6 functionality that ADCs can support include¹:

- Ability to provide IPv6/IPv4 Dual Stack for Virtual IPs (VIP)
- Server Load Balancing with port translation (SLB-PT/SLB-64) to IPv4 servers (and the ability to transparently load balance a mix of IPv4 and IPv6 servers)
- NAT64 and DNS64 (to provide IPv6 name resolution services for IPv4-only servers)
- Dual-stack Lite (DS-lite)
- SNMP IPv4 and IPv6 support for monitoring, reporting and configuration
- Ability to provide utilization and usage statistics separated by IPv4 and IPv6

Virtual ADCs

There is a wide array of options for implementing virtual ADCs. These options include:

- General Purpose VM Support
- Network Appliance O/S Partitioning
- Network Appliance with OEM Hypervisor
- Network Appliance with Custom Hypervisor

Each of these approaches has advantages and disadvantages that effect overall scalability and flexibility. General purpose VM support has the most flexibility, but when compared to network appliance hardware, general purpose VM support gives the lowest level of performance and reliability. Network appliances with custom hypervisors can provide the greatest performance levels, but provide the least flexibility with limited co-resident applications and virtualization framework support.

¹ [IPv6 Deployment Starts at Network Edge](#)

NFV Optimization

While performance bottlenecks are not unique to a virtualized environment such as an NFV environment, as IT organizations adopt a virtualized environment the performance bottlenecks multiply. Acquiring solutions that have effective packet processing software that can bypass bottlenecks is one of the primary ways to avoid experiencing unacceptable performance in a virtualized environment. When evaluating the enabling packet processing software, IT organizations should check for the following criteria in order to ensure a cost effective value proposition and a smooth transition to support future requirements:

- Equal performance in both physical and virtual environments;
- Transparency: No change should be required to the operating system, the hypervisor, the virtual switch or to the management tools;
- Availability: The solution must work across multi-vendor processors, NICs and hardware platforms.

Emerging WAN Optimization Services

Emerging Environment

In the traditional IT environment, the end users reside in a corporate office and the applications and data that the users need to access are housed in a corporate data center. While the traditional IT environment is still somewhat common, a different IT environment is becoming increasingly common. One of the key characteristics of this new environment is that the users are mobile and use a wide array of access devices. Another key characteristic of this emerging IT environment is that users are increasingly accessing applications and data that are provided by cloud service providers.

The traditional optimization appliances (e.g., WOCs and ADCs) provide significant value in an environment where the users as well as the applications and data the users are accessing are in a fixed location and under the control of the IT organization. However, a new set of optimized WAN services is emerging which is highly complementary to the traditional approach to optimization. This emerging set of solutions is focused on environments in which one or both of the end points is either not in a fixed location or not under the control of the IT organization.

Cloud-Based, Private WAN Optimization Solutions

In a cloud-based, private WAN optimization solution a variety of types of users (e.g., mobile users, branch office users) access WAN optimization functionality at the service provider's points of presence (POPs) and the POPs are inter-connected by a private WAN. Ideally a solution of this type supports a wide variety of access services. In addition, the solution must have enough POPs so that there is a POP in close proximity to the users and to the applications and data the users want to access so as to not introduce unacceptable levels of delay.

The Optimization of Internet Traffic

Throughout *The Handbook* the class of WAN optimization service that has a focus on optimizing Internet traffic will be referred to as an Optimizing Internet Traffic Service (OITS). An OITS leverages service provider resources that are distributed throughout the Internet. The way this works is that all client requests to the application's origin server in the data center are redirected via DNS to a server in a nearby point of presence (PoP) that is part of the OITS. This edge server then optimizes the traffic flow to the OITS server closest to the data center's origin server. Intelligence within the OITS servers can also be leveraged to provide extensive network monitoring, configuration control and SLA monitoring of a subscriber's application and can also be leveraged to provide security functionality.

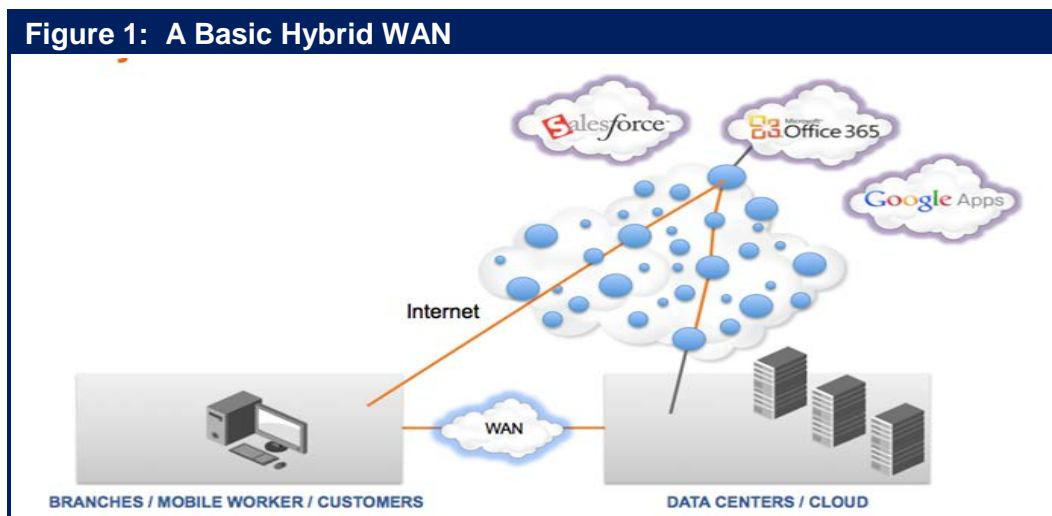
Hybrid WAN Optimization Solutions

Throughout *The Handbook* the phrase *hybrid WAN* refers to a network that is comprised of two or more WAN services such as MPLS and the Internet.

A Basic Hybrid WAN

The traditional approach to providing Internet access to branch office employees has been to backhaul that Internet traffic on the organization's enterprise network (e.g., their MPLS network) to a central site

where the traffic was handed off to the Internet. One way that a hybrid WAN can eliminate the disadvantages of backhauling traffic is shown in **Figure 1**.



In order for an IT organization to feel comfortable implementing the network shown in Figure 1, the organization must find a way to implement the security and control that it has when it backhauls Internet traffic. One way this can be done is to replace the basic Internet connection shown in Figure 1 with an OITS. The advantage of this is that in addition to providing optimization functionality, the OITS can provide the security functionality that was previously provided in the corporate data center.

The hybrid WAN that is described above is deemed to be a *basic hybrid WAN* service because it doesn't layer any additional intelligence over what is typically contained in the primary components of the service; e.g., a private WAN service such as MPLS; the basic Internet; or an OITS.

Intelligent Hybrid WANs

The preceding discussion of a basic hybrid WAN included the use of traditional Policy Based Routing (PBR) to determine which traffic transited which WAN link. One of the concerns with PBR is the static nature of the PBR forwarding policies. A relatively new class of device has emerged to address the shortcomings of PBR: A WAN path controller (WPC). A WPC works in conjunction with WAN routers to simplify PBR and to make the selection of the best end-to-end WAN path based on real-time traffic analytics.

One way to construct an intelligent hybrid WAN is to leverage WPC to apportion traffic over two WAN links where one WAN connection is a basic Internet connection and the other connection is MPLS. The added intelligence found in a WPC will improve the performance of the WAN and this WAN design alleviates at least some of the concerns about cost and uptime. Another option is to still have one WAN connection be MPLS, but instead of using the basic Internet, have the other connection use an OITS. Because of the security functionality provided in an OITS, this approach should alleviate the previously mentioned security concerns. This approach also improves performance because an OITS optimizes traffic by offloading data out of data-centers to caches in OITS servers close to the users. It is possible, however, to further leverage the intelligence of an OTIS. For example, instead of offloading data out of data-centers to caches in OITS servers, it is possible to offload data out of data-centers to caches in the branch office and hence eliminate the round-trip delay on the access links.

Management

Key Management Tasks

The Survey Respondents were asked about the importance of a range of management tasks. Their feedback indicates that:

- Two tasks are in a virtual tie for the most important management task to get better at over the next year: 1) Rapidly identifying the root cause of degraded application performance; 2) Identifying the components of the IT infrastructure that support the company's critical business applications.
- The second most important set of management tasks include: 1) Obtain performance indicator metrics and granular data that can be used to detect and eliminate impending problems; 2) Monitor the end user's experience and behavior; 3) Effectively manage SLAs for one or more business critical applications; 4) Manage the use of VoIP.

Impact of SDN

SDN creates some new management challenges. For example, one of the primary benefits of SDN is the ability to support multiple virtual networks that run on top of the physical network. Effective operations management, however, requires tools that give operators clear visibility into the relationships between the virtual and physical networks and their component devices. In addition, the SDN controller is in the data path for new flows entering the network. During periods when many new flows are being created, the controller can potentially become a performance bottleneck adding significant latency for flow initiation. Performance management systems need visibility not only into application performance but also controller performance in processing flows.

The document entitled [*Mock RFI for Enterprise SDN Solutions*](#) contains a number of questions that IT organizations should ask SDN vendors relative to SDN management.

Application Performance Management

A Framework

Since any component of a complex service such as Customer Relationship Management (CRM) can cause service degradation or a service outage, in order to effectively perform application performance management IT organizations need a single unified view of all of the components that support a service. This includes the highly visible service components such as servers, storage, switches and routers, in both their traditional stand-alone format as well as in their emerging converged format. It also includes the somewhat less visible network services such as DNS and DHCP, which are significant contributors to application degradation. Multiple organizational units within an IT organization have traditionally provided all of these service components. On an increasing basis, however, one or more network service providers and one or more cloud computing service providers will provide some or all of these service components. As a result, in order to achieve effective service delivery management, management data must be gathered from the enterprise, one or more Network Service Providers (NSPs) and one or more Cloud Computing Service Providers (CCSPs). In addition, in order to help relate the IT function with the business functions, IT organizations need to be able to understand the key performance indicators (KPIs) for critical business processes such as CRM and relate these business level KPIs to the performance of the IT services that support the business processes.

Enterprise IT organizations can choose among several types of tools for monitoring and managing application performance over a private enterprise network. These include: application agents, monitoring of real and synthetic transactions, network flow and packet capture, analytics, and dashboard portals for the visualization of results.

At a high level, there are two basic classes of tools. The first class of tool monitors global parameters such as user response time or transaction completion time and provides alerts when thresholds are exceeded. These tools include agents on end user systems and monitoring appliances in the data center. The second class of tool supports triage by monitoring one or more of the components that make up the end-to-end path of the application. These tools include devices that capture application traffic at the flow and packet levels, agents on database, application, and web servers, as well as agents on various network elements.

Application Aware Network Performance Management

In response to the fact that enterprise networks and the applications that transit these networks are becoming increasingly entwined, there has been a movement to bring together two management disciplines: Application Performance Management and Network Performance Management. The result of bringing together those two disciplines is a new discipline that is often referred to as [Application Aware Network Performance Management \(AANPM\)](#). An AANPM solution integrates data that has historically been associated with application performance management with data that has historically been associated with network performance management. The result is a system that provides cross-platform visibility that enables IT organizations to monitor, troubleshoot and analyze both network and application systems.

DevOps

The phrase *DevOps* is a result of bringing to together two phrases: *Development* and *Operations*. That's appropriate because the point of adopting DevOps is to establish tight collaboration between a number of the phases of the application development lifecycle, including application development, testing, implementation and ongoing operations. DevOps is not a technology, but an approach. Some of the key characteristics of the approach are that the applications development team writes primarily small incremental pieces of code that are tested on an architecture that reflects the production architecture. Ideally, the network on which the software is tested will reflect not just the architecture but also the same characteristics (i.e., delay, packet loss) as the production network.

Implementing DevOps provides many advantages. For example, DevOps can provide business value by enabling companies to experience sustained innovation². Examples of companies that claim to have experienced sustained innovation as a result of implementing DevOps include Twitter, Netflix and Facebook. Implementing DevOps has other advantages. According to a recent [Information Week Report](#), eighty two percent of the IT organizations that implemented DevOps saw at least some improvement in infrastructure stability and eighty three percent saw at least some improvement in the speed of application development.

² [Use DevOps to Turn IT into a Strategic Weapon](#)

Security

The Changing Security Landscape

The security landscape has changed dramatically in the last few years. In the very recent past, the typical security hacker worked alone, relied on un-sophisticated techniques such as dumpster diving, and was typically motivated by the desire to read about their hack in the trade press. In the current environment, sophisticated cyber criminals have access to malware networks and R&D labs, can rent botnets, and can use these resources to launch attacks whose goal is often to make money for the attacker. In addition, national governments and politically active hackers (hacktivists) are engaging in cyber warfare for a variety of politically motivated reasons.

IT security systems and policies have evolved and developed around the traditional application delivery architecture in which branch offices are connected using a private WAN service to application servers in a central corporate data centers. In this architecture, the central corporate data center is a natural location to implement IT security systems and policies that provide layered defenses as well a single, cost efficient location for a variety of IT security functions. With the adoption of public cloud computing, applications and services are moving out of the central corporate data center and there is no longer a convenient single location for security policies and systems.

In addition, IT security systems and policies have traditionally distinguished between people who were using IT services for work versus those who were using it for personal use. The use of an employer provided laptop was subject to the employer's IT security policies and systems. In this environment, the use that employees made of personal laptops was generally outside of the corporate IT security policy. With the arrival of smartphones and tablet computers, the ownership, operating systems and security capabilities of the end user devices have changed radically. IT security policies and standards that were developed for PCs are no longer effective nor optimal with these devices. Most corporations have embraced the BYOD movement and end users are less willing to accept strict corporate security policies on devices they own. Additionally, strict separation of work and personal usage for security on an employee owned device is impractical.

Current State of DDoS Attacks

A number of recent reports have highlighted the evolving threats that are associated with DDoS attacks on data centers. One of the key findings of those reports is that DDoS attacks are growing in a variety of ways, including:

- Frequency: A 50% increase in DDoS attacks on a year-over-year basis³;
- Size: One attack out of three is over 20 Gbps, 60 Gbps attacks are common and 100 Gbps attacks are not uncommon⁴;
- Persistence: The average duration of a DDoS attack is 17 hours⁵.

³ [Akamai's State of the Internet 2014](#)

⁴ [Neustar Annual DDoS Attacks and Impact Report](#)

⁵ [Prolexic Global Attack Report Q1 2014](#)

Web Application Firewall Services

Roughly twenty years ago IT organizations began to implement the first generation of network firewalls. These devices were placed at the perimeter of the organization with the hope that they would prevent malicious activities from causing harm to the organization.

Whereas network firewalls are focused on parameters such as IP address and port numbers, a more recent class of firewall, referred to as a Web application firewall, analyzes messages at layer 7 of the OSI model. Web application firewalls are typically deployed as a hardware appliance and they sit behind the network firewall and in front of the Web servers. In some cases, Web application firewall functionality is provided by an Application Delivery Controller (ADC).

Web application firewalls look for violations in the organization's established security policy. For example, the firewall may look for abnormal behavior or signs of a known attack. It may also be configured to block specified content, such as certain websites or attempts to exploit known security vulnerabilities. Because of their ability to perform deep packet inspection at layer 7 of the OSI model, a Web application firewall provides a level of security that cannot be provided by a network firewall.

In order to be effective, a Cloud Based Security Solution (CBSS) that provides Web application firewall functionality needs to be deployed as broadly as possible, preferably in thousands of locations. When responding to an attack, the service must also be able to:

- Block or redirect requests based on characteristics such as the originating geographic location and whether or not the originating IP addresses are on either a whitelist or a blacklist.
- Direct traffic away from specific servers or regions under attack.
- Issue slow responses to the machines conducting the attack. The goal of this technique, known as tarpits⁶, is to shut down the attacking machines while minimizing the impact on legitimate users.
- Direct the attack traffic back to the requesting machine at the DNS or HTTP level.

Impact of SDN

As was the case with management, SDN poses both security challenges and security opportunities. The primary security challenge is to ensure that an attacker cannot compromise the central SDN controller and hence have access to all of the subtending network elements. In addition to securing the controller itself, all communication between the controller and other devices including switches, network services platforms and management systems must be secured.

As noted, SDN also presents opportunities to improve security by implementing security related applications that leverage the control information that has been centralized in the SDN controller. One such application that has been announced⁷ is a network service that provides DDoS protection. Another such example is an application⁸ that was designed to combat the security challenges that are associated with BYOD.

The document entitled [Mock RFI for Enterprise SDN Solutions](#) contains a number of questions that IT organizations should ask SDN vendors relative to security.

⁶ Wikipedia Tarpit(networking)

⁷ Radware: DefenseFlow

⁸ HP Network Protector SDN Application

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

Jim Metzler has a broad background in the IT industry. This includes being a software engineer, an engineering manager for high-speed data services for a major network service provider, a product manager for network hardware, a network manager at two Fortune 500 companies, and the principal of a consulting organization. In addition, he has created software tools for designing customer networks for a major network service provider and directed and performed market research at a major industry analyst firm. Jim's current interests include cloud networking and application delivery.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact [Jim Metzler](#) or [Steven Taylor](#).

**Published by
Webtorials
Editorial/Analyst
Division**
www.Webtorials.com

Division Cofounders:
Jim Metzler
jim@webtorials.com
Steven Taylor
taylor@webtorials.com

Professional Opinions Disclaimer

All information presented and opinions expressed in this publication represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.

Copyright © 2014 Webtorials

For editorial and sponsorship information, contact Jim Metzler or Steven Taylor. The Webtorials Editorial/Analyst Division is an analyst and consulting joint venture of Steven Taylor and Jim Metzler.



Packet Processing Software

Increase Data Plane Performance
No Change To Linux Environments
Available Across All Major Platforms
Support Extensive Set Of Protocols

L2-L4 Acceleration
IPsec VPN Gateways
TCP / UDP Termination
Virtual Switching
DPDK
And More ...

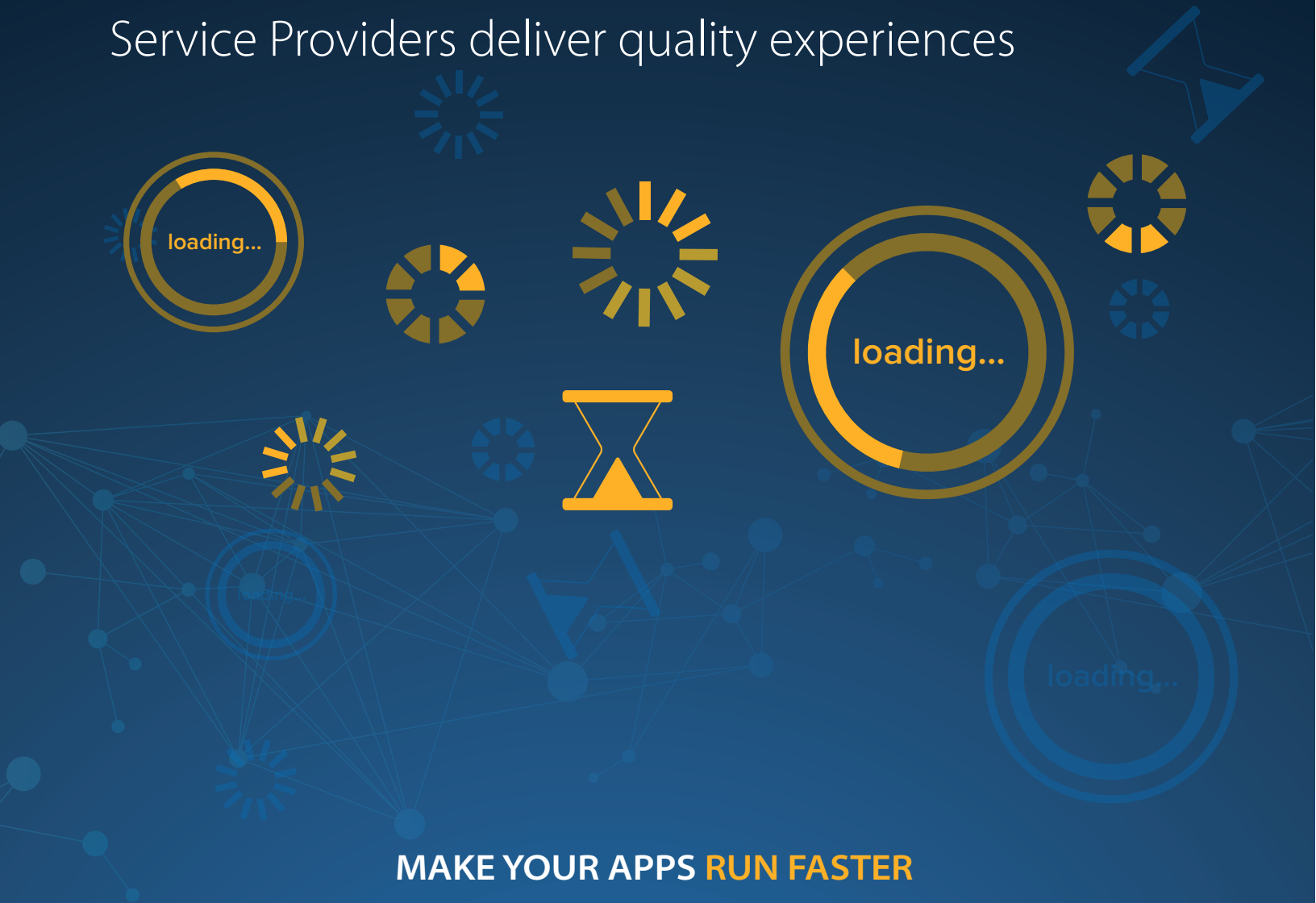


6WIND.com
SPEED MATTERS



ARE YOUR USERS **WAITING** **MORE THAN DOING?**

A10 helps more than 3,000 Enterprises and Service Providers deliver quality experiences



MAKE YOUR APPS **RUN FASTER**

Experience the Performance

www.a10networks.com

Enterprises today aspire to grow revenue by expanding globally and acquiring new customers, while also cutting costs and finding ways to become more agile. To realize their goals, every Enterprise has a core set of applications that they rely on to run their business operations.

Current Application Delivery Landscape

The user requirements for accessing and business applications is changing dramatically, and Enterprises must support more applications across a broader user base including customers, suppliers, partners, and employees. In order to leverage their applications to achieve their business goals, Enterprises must optimize the delivery of their applications to support fast, reliable, and secure access to ensure all users, both inside and outside of their organization, have the best possible experience.

In the past, Enterprises would resort to optimizing their application delivery using a physical hardware box or a virtual appliance that was deployed within a data center and any offices where users were located. While costly to deploy and manage, this approach did a good job of optimizing application delivery between the data center and branch office locations that were connected via a private network. Today, this approach is no longer effective due to several factors including:

- The complexity of having more users outside the organization's private network
- Applications distributed across multiple data centers and in the cloud
- End-users located all over the world using all sorts of different devices and networks, and
- A growing list of critical business applications such as CRM, collaboration, product lifecycle management, and support portals that users rely on every day.

It's not realistic for IT organizations to establish private network connections between all their users and all the data centers where their applications are hosted, or implement an application delivery box or virtual appliance in every data center, cloud environment, and every location where their end-users are located today.

In order to leverage their applications to achieve their business goals, organizations today cannot only rely exclusively on their private WAN to deliver their applications, but they must also leverage the ubiquity and scale of the Internet in order to embrace the trends of globalization and consumerization within their organizations.

Considering Akamai's Cloud-based Application Delivery Platform

Akamai's Terra Alta solution is a cloud-based Application Delivery Platform that enables Enterprises to leverage the Internet to deliver all their web-based applications in a fast, reliable, secure, and cost-effective way. Terra Alta is a managed service that empowers Enterprises to overcome the challenges related to delivering their applications over the Internet by placing all of the application delivery capabilities within Akamai's cloud-based Intelligent Platform, instead of requiring IT organizations to take on the burden of deploying and managing these critical capabilities on their own in the form of hardware boxes or virtual appliances. With Akamai, application optimizations are distributed globally across our Intelligent Platform, not constrained within the four walls of a few data centers, or restricted only to those users on a private network connection.

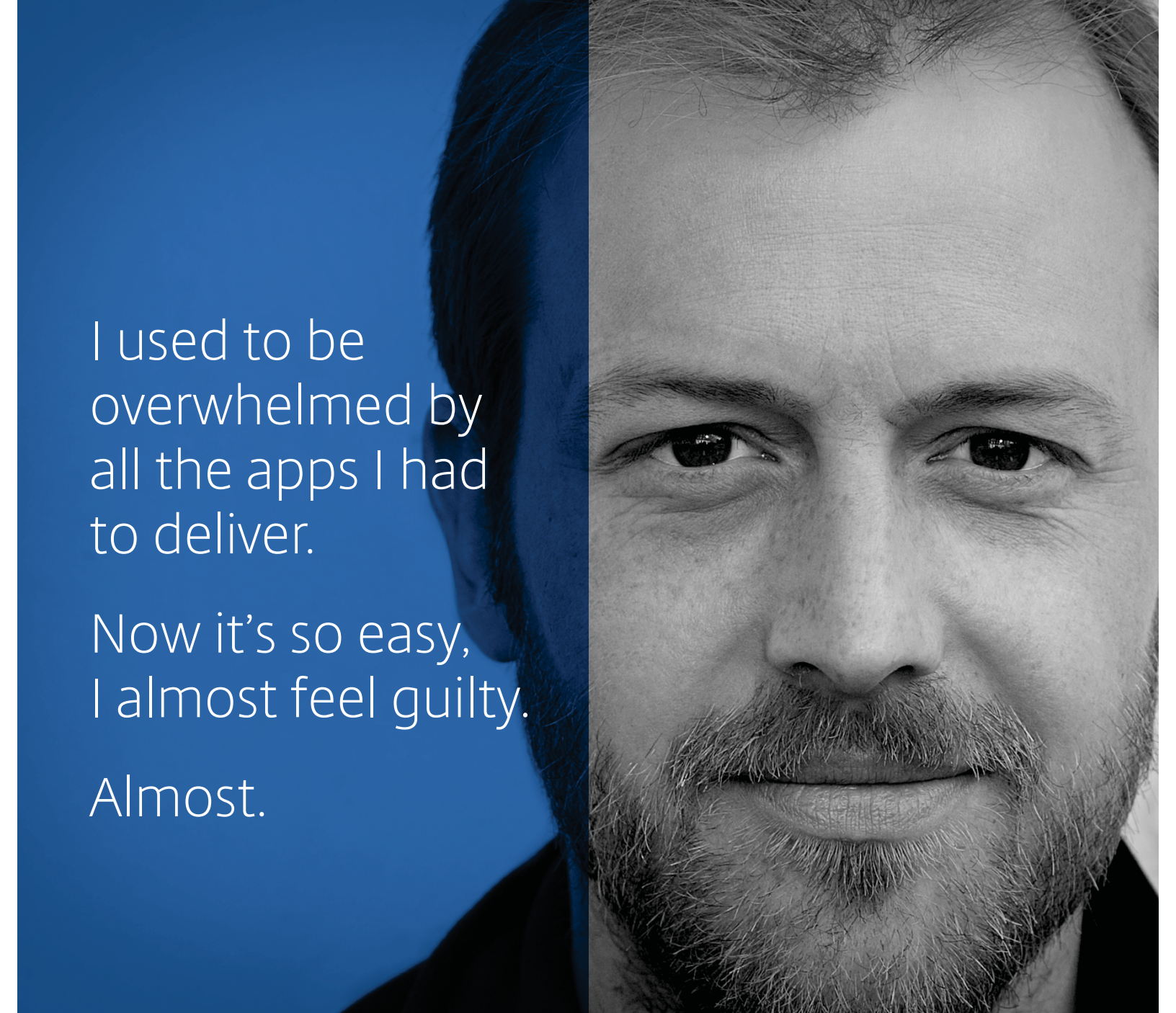
Akamai's Intelligent Platform is deployed on over 150,000+ servers which are embedded deeply into thousands of networks worldwide, which means we are very close to nearly all of the world's Internet users and datacenters. This means that users can benefit from fast, reliable, and secure business applications regardless of where they are located in the world! In addition to being a cloud-based platform, Akamai is device agnostic and does not require any application changes, which means it's quick and easy to implement and allows organizations to lower their IT costs and reduce complexity as compared to alternative application delivery optimization solutions. Akamai's unique cloud-based architecture also means that applications can be seamlessly migrated across data centers or cloud providers at will, and the application delivery optimizations will automatically move with the application. Terra Alta empowers Enterprises to embrace their cloud, mobile, and big data initiatives without the fear of increased costs or low application adoption.

Conclusion

By overcoming the new realm of global application delivery challenges, Akamai's cloud-based Application Delivery Platform empowers organizations to meet the demands of globalization and consumerization and instantly enter new markets, acquire new customers, improve customer interactions, do business via lower-cost online channels, enable end-users to get more done in less time, and achieve their goal of increasing revenue and reducing costs.

We make the Internet fast, reliable, and secure.





I used to be
overwhelmed by
all the apps I had
to deliver.

Now it's so easy,
I almost feel guilty.

Almost.

NetScaler with TriScale harnesses the power
of software so you can effortlessly customize
your app delivery for any business need.



NetScaler with TriScale
SOFTWARE SMART. HARDWARE STRONG.

CITRIX®

www.citrix.com/netscaler



City Index

NetScaler reduces expenses with data center consolidation

City Index (www.cityindex.co.uk), is a leading global provider of retail trading services, including Spread Betting (UK only), Contracts for Difference (CFDs) and margined foreign exchange (FX). With offices in London (HQ), Warsaw, Tel Aviv, Singapore, Sydney and Shanghai, City Index supports its global clients on various trading platforms running on multiple backend applications. City Index is committed to providing a market-leading client service, transparent prices and innovative technology. All IT operations are centralized from two datacenters in London and one in Florida.

The challenge: need for a cost effective application delivery controller

Marc Morgan-Davies, Infrastructure Manager for City Index explained, our existing load balancing F5 solution that consisted of six BIG-IP 3400s and eight BIG-IP 6400s reached the end of support. There were two legacy Citrix Access Gateways (CAG) that we wanted to replace as well. We wanted a more cost effective and consolidated solution for our two London datacenters with an extended feature set that included global load balancing, DNS responder and rewrite, SSL offload, compression and caching.

Our choices were F5, Citrix, A10 Networks and Riverbed and we narrowed it down to F5 VIPRION 4400 and Citrix NetScaler 11500 SDX based on features and reputation. Our emphasis for the solution was more on the available feature set rather than raw processing power due to the nature of our platforms. The licensing model employed by Citrix is much simpler and more cost effective in my opinion than the competitors. For instance, if you want to enable a fourth module on the F5 you require another physical blade.” Marc Morgan-Davies continued, “NetScaler on the other hand provided all of our required features on a single appliance with a simpler licensing model as well as allowing us to consolidate the existing CAGs onto the new devices further reducing our physical footprint and operating expenses. NetScaler gave us more features at a lower cost so was our chosen solution.”

The solution: NetScaler SDX

Citrix NetScaler is an Application Delivery Controller (ADC) that optimizes the security, availability, scalability and performance of web-based applications and is available as a physical or virtual appliance. Citrix NetScaler

Industry:

Financial Services

Key Benefits:

- Reduces capital and operating expenses
- Provides an extended feature set on demand
- Ensures uninterrupted availability of trading platforms and applications

Citrix Products:

- Citrix NetScaler SDX
- Citrix NetScaler VPX

SDX is a true service delivery networking platform for enterprises and cloud datacenters. NetScaler SDX provides an advanced virtualized architecture that supports multiple NetScaler instances on a single hardware appliance, while an advanced control plane unifies provisioning, monitoring and management to meet the most demanding multi-tenant requirements.

NetScaler VPX is a software-based virtual appliance built for cloud scale. As an easy-to-deploy application delivery solution that runs on multiple virtualization platforms, the simplicity and flexibility of NetScaler VPX make it simple and cost-effective to fully optimize every web application and more effectively integrate networking services with application delivery. Performance capacities can be upgraded in production with the simple addition of a pay-as-you-grow license. NetScaler VPX helps organizations control costs by leveraging processing capacity already in place, including existing virtualized servers and associated resources.

“In October 2012, we installed 2 NetScaler SDXs as HA pair in production in each of our London datacenters. Each SDX box have 2 VPX instances that have discrete security layers. In addition, we installed 2 SDXs as HA pair for staging in London with each SDX running 9 VPX instances. We are extremely pleased with NetScaler’s ease of configuration and use.” said Morgan Davies.

Key benefit: reduces capital and operating expenses

Using NetScaler we were able to prevent appliance sprawl by upgrading and consolidating 14 F5 Big-IP appliances and 2 Citrix Access Gateways to just 6 Citrix NetScaler appliances. This helped reduce support costs, rack space, ongoing power and cooling requirements drastically.” Marc Morgan-Davies emphasized.

Key benefit: provides an extended feature set on demand

According to Marc Morgan-Davies, “Citrix NetScaler helped upgrade infrastructure while controlling costs. NetScaler provided the complete ADC feature set we required with the ability to enable features on demand.”

Key benefit: ensures uninterrupted availability of trading platforms and applications

NetScaler ensured 24X7 availability of City Index’s trading platforms and applications by providing global load balancing and SSL offloading between the London datacenters.

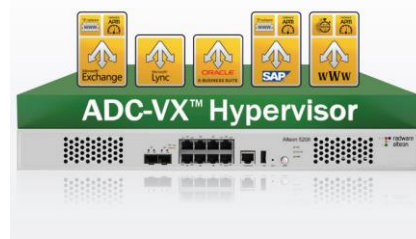
Looking ahead to the future

“NetScaler is a requirement to deploy Citrix XenMobile and MDM that would satisfy our requirement for a secure solution for users to access the corporate resources from any location using any device. Citrix mobility technologies are now very much on our scope for implementation in the near future. We are also looking into NetScaler App Firewall feature as well.” Marc Morgan-Davies concluded.

About Citrix

Citrix (NASDAQ:CTXS) is the cloud company that enables mobile workstyles—empowering people to work and collaborate from anywhere, easily and securely. With market-leading solutions for mobility, desktop virtualization, cloud networking, cloud platforms, collaboration and data sharing, Citrix helps organizations achieve the speed and agility necessary to succeed in a mobile and dynamic world. Citrix products are in use at more than 330,000 organizations and by over 100 million users globally. Annual revenue in 2012 was \$2.59 billion. Learn more at www.citrix.com.

©2014 Citrix Systems, Inc. All rights reserved. Citrix®, NetScaler®, SDX™, VPX™ XenMobile and App Firewall are trademarks or registered trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.



Predictable Application SLA, Guaranteed. Only with Alteon NG.

Whether it's an online web application, or an internal mission-critical enterprise application such as CRM, ERP, or an organizational portal, end-users expect to receive the same, unchanged quality of experience. The conclusion is clear: today's organizations require **predictable application SLAs** and need tools to proactively monitor and manage application SLAs.

The Standard ADC: Not Good Enough Anymore

For years, companies have been using application delivery controllers (ADC) to optimally deliver applications. However, the standard/legacy ADC is not enough anymore as it is based on a **best-effort approach**.

In contrast to the legacy ADC, a **next-generation (NG) ADC** can provide full application SLA assurance through reserving resources per application. This allows the addition of new services without performance penalty and the inclusion of real-user monitoring, best-in-class application-level acceleration features and an innovative security offering.

Alteon NG: Complete Application SLA Assurance

The Alteon® next-generation (NG) ADC solution is the industry's only ADC built from the ground up to ensure application SLAs at all times. It innovatively leverages several next-generation services that are not available in any other ADC on the market:

- ☑ Alteon NG is **architecturally designed to ensure application SLA** by delivering full resource isolation per application, service, or department. Each virtual ADC (vADC) instance is completely isolated from neighboring instances with independent CPU cores, memory, network stack, management control, and operating system. Our unique solution is designed to dynamically scale to add more throughput, services, and vADCs without hardware modification resulting in fast provisioning of additional vADC instances and no service degradation, interruption, or resource overcapacity.
- ☑ Radware's **Application Performance Monitoring (APM)** module provides real-time tracking of application SLAs by measuring real-user transactions and errors. Embedded in Alteon NG, Radware's APM is an out-of-the-box solution which doesn't require synthetic transaction scripting or additional installation - reducing deployment time and costs. Radware's APM intuitively tracks SLA by location, user, application and transaction type to expedite root cause analysis. In addition, it provides historical reports based on user-defined SLA that feature granular analysis allowing the measurement of the delay per transaction phase including data center time, network latency and browser rendering time.
- ☑ Alteon NG integrates FastView® the industry's most advanced **Web Performance Optimization (WPO)** technology – which accelerates application response by up to 40% – for higher conversion rates, revenues, productivity, and customer loyalty. FastView acceleration treatments are optimized according to each user, end-user device and browser - with specific optimization for mobile devices. In addition, FastView automatically optimizes new applications,

new application versions and new application modules – reducing manual code optimization while letting you focus on core business competencies.

- ☑ Alteon NG is part of Radware's unique **Attack Mitigation System (AMS)**, which enables accurate detection and mitigation of the most advanced cyber-attacks. Leveraging a unique Defense Messaging™ mechanism, AMN efficiently mitigates attacks by signaling attack information to Radware DefensePipe cloud service and Radware DefensePro data center attack mitigator, located in the cloud or the network perimeter, respectively.
- ☑ Integrating advanced **Web Application Firewall (WAF)** capabilities, Alteon NG enables risk-free implementation thanks to a unique out-of-path WAF deployment mode along with auto-policy generation capabilities. Moreover, as ADC resources are ensured via full instance isolation and resource reservation, even when WAF policies are updated there's no impact on application availability and performance. This results in secured web applications with SLA guarantee.
- ☑ Alteon NG features a built-in authentication gateway with **Single Sign On (SSO)** capabilities by supporting Radius, Active Directory, LDAP and RSA SecurID – simplifying the user experience without compromising on application security.
- ☑ Alteon NG employs Radware's **AppShape™** offering configuration templates for leading business applications (e.g. Microsoft, Oracle, SAP). This helps customers roll out ADC-optimized applications in a simple, fast risk-free manner. In addition, Radware's AppShape++ scripting technology lets customers customize any ADC service per specific application flow/scenario. Using the AppShape++ script library, customers can refine various Layer 4-7 policies including HTTP, HTTPS, TCP, UDP, SSL and more – without application modifications to reduce cost and risk.

Complete Load Balancing/Layer 4-7 Feature Set

Alteon NG delivers a complete set of layer 4-7 services to ensure the availability, performance and security of mission-critical applications in the local and cloud data centers. These extend to traffic redirection, content modification, persistency, redundancy, advanced health monitoring and global server load balancing (GSLB). In addition, Alteon NG integrates advanced modules such as bandwidth management and link load balancing – reducing data center footprint and simplifying deployment. The combination of these advantages – along with an industry unique 5-year longevity guarantee, “pay-as-you-grow” approach in throughput, number of vADCs and services, plus performance leadership in all layer 4-7 metrics – makes Alteon simply your best application delivery choice.

Want to see more for yourself? We invite you to download our Radware ADC solution white paper [here](#) or contact us at: info@radware.com.