The Mandate for Converged Packet Visibility

Ashton, Metzler & Associates

Leverage Technology & Talent for Success

Introduction

A recent article, *Digital Business Strategy: Toward a Next Generation of Insights*[1], discussed how the movement to implement digital business initiatives impacts IT organizations. According to that article,

> "Digital technologies (viewed as combinations of information, computing, communication, and connectivity technologies) are fundamentally transforming business strategies and business processes. Accordingly, we argue that the time is right to rethink the role of IT strategy, from that of a functional-level strategy — aligned but essentially always subordinate to business strategy — to one that reflects a fusion between IT strategy and business strategy. This fusion is herein termed **digital business strategy**."

Independent of how much progress a company has made relative to transitioning to become a digital business, there is no doubt that the majority of companies are seeing an ever increasing blurring of the distinction between their business processes and their IT functionality. One result of this blurring is that if the IT infrastructure is not performing well, neither are the company's business processes.

Another result of this blurring is that security intrusions can have a dramatic impact on a company's profitability. That fact was demonstrated when Target suffered a large security intrusion that resulted in Target's profits dropping by almost 50%[2]. Because of the growing impact that a company's IT infrastructure has on it business processes and overall profitability, an effective digital business strategy must refocus on how to monitor the performance and security of the infrastructure. Because of the role it plays housing applications and data, a company's data center is the most critical component of the company's IT infrastructure. Ironically, just at the time when a company's business processes increasingly depend on the performance and security of the company's data centers, a number of technological trends are causing data centers to evolve dramatically, which makes the task of monitoring the performance and security of data centers significantly more difficult.

This white paper aims to:

- Describe some of the technological trends that are making the task of monitoring the data center so much more challenging.
- Discuss the organizational impact of the mandate to focus equally on the IT infrastructure as well as on how to effectively monitor the performance and security of the infrastructure.
- Identify the need for a converged approach to network monitoring and security.

---

[1] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2742300

[2] http://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/#1148324e5e8c

- Describe how NETSCOUT's unified packet plane[3] approach enables an IT organization to overcome the challenges that are associated with the evolving data center and effectively monitor the performance and security of their company's IT infrastructure.

Technological Trends Driving Change

The technological trends described below are making the task of monitoring the performance and security of the data center significantly more difficult:

Increasing sophistication of security intrusions

It is difficult to read a business journal and not see an article that describes a new, highly sophisticated security intrusion. A statement in the *IBM X-Force Threat Intelligence Report 2016*[4] underscores the general trend of such intrusions: "It is safe to say that we have never before seen the magnitude and sophistication of online crime as we did in 2015—a trend that's already proving to persist into 2016." That report also predicted that by 2019 cybercrime will become a $2.1 trillion problem.

One of the primary reasons why security intrusions are becoming continually more sophisticated is because hackers themselves are becoming more sophisticated. According to an article at the security and risk management site CSO[5], "Today, the average age of a cyber-criminal is 35, and 80% of black-hat (e.g., criminal) hackers are affiliated with organized crime. In other words, people are choosing this as a profession. That's a radical shift, and it's led to the creation of increasingly sophisticated criminal organizations that operate with the professionalism, discipline, and structure of legitimate enterprises."

Adoption of Software Defined Networking

According to the Open Networking Foundation (ONF)[6], the Software-Defined Networking (SDN) 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 last few years have seen a lot of discussion of SDN but not much deployment. A number of recent articles have indicated that that situation is about to change. One recent article[7] pointed out that 13% of companies have already implemented SDN while another[8] predicted that by 2020 the annual revenue of the worldwide datacenter SDN market would be $12.5 billion.

Implementation of new, higher-speed data center designs

[3] http://finance.yahoo.com/news/netscout-enables-deep-packet-visibility-143000976.html
[4] http://www-03.ibm.com/security/xforce/downloads.html
[5] http://www.csoonline.com/article/2938529/cyber-attacks-espionage/cybercrime-much-more-organized.html
[6] https://www.opennetworking.org/sdn-resources/sdn-definition
[7] http://www.zdnet.com/article/research-sdn-usage-growing-in-the-enterprise/
[8] https://www.idc.com/getdoc.jsp?containerId=prUS41005016

The volume of data traffic is exploding: according to Cisco[9], global IP traffic will increase nearly threefold over the next 5 years. That is why over the last two decades the speed of data center Ethernet links has increased by a factor of 4,000 from 10 Mbps to 40 Gbps. Due to traffic volumes, in the very near future it will be common to have data center Ethernet links running at 100 Gbps.

In part to support increasing traffic loads, many network organizations have implemented a leaf-spine data center design. As shown in Figure 1, this design is comprised of leaf switches which connect to servers and storage and spine switches which connect leaf switches.

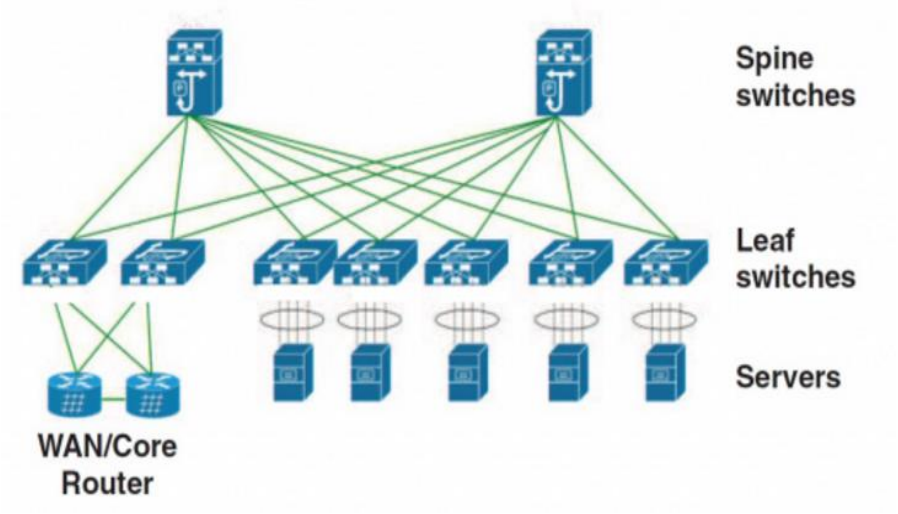

Figure 1: Leaf-Spine Network Design

Growing use of virtualization

In the traditional data center, functionality such as compute and networking are implemented in hardware-based appliances and each appliance is dedicated to a single service or application. This approach results in stranded capacity and extra cost. Another characteristic of the traditional data center is that each appliance is individually configured on a manual basis. This results in tasks such as provisioning and change management being very time consuming and error prone.

Driven by the general pressure to become more efficient and agile, over the last several years IT organizations have been adopting a variety of forms of virtualization, most notably server virtualization. However, some forms of network virtualization pre-date server virtualization. Virtual LANs (VLANs), for example, have been widely deployed for almost two decades. The advent of SDN has spawned a new way of implementing network virtualization by using techniques such as encapsulation and tunneling to construct multiple virtual network topologies that are overlaid on a common physical network.

[9] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

Another part of the movement away from hardware-specific solutions and towards software-specific solutions is the emerging adoption of Network Functions Virtualization[10] (NFV). As part of NFV, L4 – L7 functionality such as optimization and security are implemented in software running on commodity hardware. However, dedicated hardware sometimes provides value and hence the movement to software-based solutions comes with some potential performance challenge. For example, virtualization may lead to abnormal latency variations and significant throughput instability.[11]

Network Automation

As mentioned, a key characteristic of the traditional approach to designing a data center is that each appliance is individually configured on a manual basis. In order to understand the complexity that manual configuration of data center appliances entails, consider Quality of Service (QoS). Some of the primary components of QoS are:

- Packet classification to partition the network traffic into multiple priority levels;
- Congestion avoidance techniques to circumvent congestion before it becomes a problem;
- Traffic shaping mechanisms to control the flow of outbound traffic on one more interfaces.

The complexity of configuring QoS comes from the fact that there are so many components of QoS and all of them have to be configured on each of the network elements in the end-to-end data path. That complexity is made worse by the fact that in the majority of times configuring network functionality such as QoS is done using a command line interface. Driven in part by the adoption of new networking architectures such as SDN, which centralizes management and enables programmatic control of the network, and in part by the adoption of new processes, such as DevOps, network organizations are automating a range of management tasks such as configuring QoS.

Increasing number and type of security and performance monitoring tools

The last several years has seen the development of a huge range of "best of breed" monitoring tools that are focused on virtually every possible operational function that a business could have. For example, the majority of enterprises have more than 10 monitoring tools in production.[12]

While some of the proliferation of tools can be attributed to systems that are applicable only to a relatively narrow areas of focus, a number of reports have discussed the fact that there has been a proliferation of tools in traditional areas such as Customer Experience Management (CEM), Network Performance Management (NPM) and Application Performance Management (APM).

[10] https://www.sdxcentral.com/nfv/definitions/whats-network-functions-virtualization-nfv/
[11] http://web2-clone.research.att.com/export/sites/att_labs/techdocs/TD_101400.pdf
[12] https://www.moogsoft.com/whats-new/blog/vendor-proliferation-in-it-monitoring/

For example: CIOReview[13] identified the top 20 CEM providers; ProfitBricks[14] identified the top 40 APM tools; and Livewire[15] identified the top 100 network security tools.

The Organizational Impact

Because of the large and growing impact that a company's IT infrastructure has on it business processes, IT organizations have a mandate to create an effective digital business strategy that focuses equally on the IT infrastructure *and* on how to effectively monitor its performance and security.

According to Cisco[16], the movement to adopt digital business initiatives combined with technological changes such as automation and virtualization shifts the focus of the network organization from building networks to orchestrating the services that run on those networks. The role of network professionals is changing accordingly. Cisco believes that network professionals will spend more time on activities such as network analytics, optimization and proactive management tasks. These types of activities require IT organizations to be able to effectively monitor the IT infrastructure.

A recent Cisco blog[17] discussed the importance of network security monitoring as part of a company's overall security strategy. 42 percent of the people Cisco surveyed said they "used network security monitoring for proactive querying of the network – really hunting for suspicious behavior. We see more and more organizations, especially large ones, investing in hunting capabilities."

Effective security monitoring requires deep packet visibility. For example, the typical Intrusion Detection System (IDS) requires five or more packets in a stream in order to recognize the signature of an attack. If any packets are missing, the IDS is likely to not identify the attack.

One approach to network monitoring relies on using a protocol such as NetFlow to monitor network flows. When troubleshooting, NetFlow can help to answer questions such as where did the traffic originate and what application was impacted. Unfortunately, NetFlow doesn't provide real-time insight into the operations of the network. Also, while NetFlows supplies data about application usage, it lacks data about application performance. In addition to these limitations, in order to perform granular troubleshooting of complex IT environments, network professionals need access to packet-level data. For example, if a VoIP calls were entering and exiting on different ports, this would cause the quality of the call to degrade and flow-level data would not be able to recognize this misconfiguration.

The Impact of the Changing Environment on Monitoring and Security

[13] http://customer-experience-management.cioreview.com/vendors/most-promising-cem-solution-providers-of-2015.html
[14] https://blog.profitbricks.com/application-performance-management-tools/
[15] https://www.lifewire.com/insecure-org-top-100-network-security-tools-2487293
[16] https://clnv.s3.amazonaws.com/2015/usa/pdf/BRKCRT-1601.pdf
[17] http://blogs.cisco.com/security/the-true-value-of-network-security-monitoring

As an IT organization evolves its data center to accommodate the previously discussed technological trends, it must simultaneously architect and implement a packet flow visibility platform that enables the organization to effectively monitor the performance and security of the infrastructure. In order to accomplish that goal, IT organizations need to understand the impact that those trends are having on visibility. That impact is:

- The increasing sophistication of security intrusions means that IT organizations need to place continually increasing emphasis on ensuring effective security.
- The dramatic growth in IP traffic and the speed of data center links stresses the ability of monitoring tools to process all of the traffic.
- On a going forward basis the vast majority of traffic will be ad hoc voice and video and this traffic is very difficult to characterize.
- Driven in part by the adoption of new networking architectures such as SDN and in part by the adoption of new processes such as DevOps, network organizations are automating a range of management tasks.
- The ongoing adoption of network virtualization means that an increasing amount of traffic transits encrypted tunnels which makes it difficult to manage and/or secure this traffic.
- The increasing number and type of security and monitoring tools complicates the task of ensuring that the right traffic gets to the appropriate devices.

The Need for Converged Packet Visibility

In most instances the way that an organization's use of a technology evolves is that it is first introduced into an organization on a case-by-case basis driven by a specific need. There is typically little if any thought given to how to provide the functionality at scale. However, once the deployment of the technology reaches a critical mass, it is common to converge multiple separate instances of the technology onto a single, highly-scalable instance of the technology. An example of this phenomena is databases. Databases were initially deployed on an application-by-application basis, but now most companies have converged their disparate databases onto an SQL cluster. It used to be common for each department in a company to create and manage their own Web page. Today most companies have converged those disparate Web pages onto a centralized Web portal.

In order to mitigate the challenges described in the preceding section, IT organizations must deploy a visibility platform that follows the same evolutionary path as did databases, Web pages and countless other technologies. That means that IT organizations must converge their current silos of visibility that are based on a large and growing number of different types of performance monitoring and security systems onto a unified packet plane as described below.

In addition to converging multiple performance monitoring and security systems onto a unified packet plane, the visibility platform must achieve the following goals:

- Scale to support continually higher speed links and a growing number of monitoring devices without losing any data.
- Have the capability to access packet level data at full line rate.
- Have the capability to fully analyze traffic in real-time and make appropriate decisions based on that analysis.

NETSCOUT's unified packet plane approach satisfies the mandate to converge the current silos of visibility and it also achieves the goals listed above. As shown in Figure 2, one of the key architectural principles of this approach is that it logically separates the network from the monitoring and/or security systems. One of the many advantages of this approach is that the resulting packet plane can monitor both the physical and virtual components of the infrastructure. It also enables the network organization to make changes to the network without having those changes impact the monitoring and/or security systems.

In order to overcome the type of latency and throughput challenges that were highlighted in *Network Functions Virtualization: Challenges and Opportunities for Innovations*[18], another key architectural principle of a unified packet plane is that some computationally intensive activities, such as processing encapsulated traffic and eliminating duplicated packets, are performed in dedicated hardware. Using dedicated hardware enables these activities to occur at wire speed and is in contrast to software-based solutions which tend to experience reduced capacity when each additional feature is turned on. NETSCOUT's solution offers both dedicated hardware and large buffers; thus, unlike platforms that don't have those capabilities, NETSCOUT's platform can mitigate the effects microbursts of traffic without dropping packets.

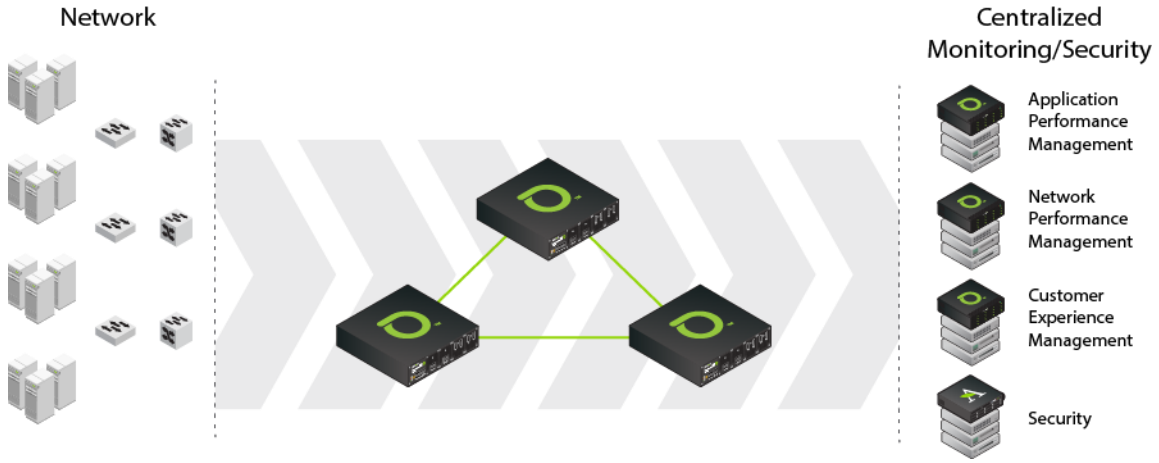

Figure 2: NETSCOUT's Unified Packet Plane

As is also shown in Figure 2, the NETSCOUT unified packet plane removes the traditional silos of visibility and it scales a company's monitoring infrastructure by employing a self-organizing

[18] http://web2-clone.research.att.com/export/sites/att_labs/techdocs/TD_101400.pdf

mesh of nGenius® packet flow switches[19]. Similar to some other visibility platforms, NETSCOUT's packet flow switches send legitimate "test", or health check, packets to the monitoring and security systems. If those packets are returned, the platform knows that the systems are available. One of the unique feature of NETSCOUT's visibility platform is that it also sends known illegitimate health check packets to the monitoring and security systems. If those packets are returned then the platform knows that the systems appear to be available, but they are not functioning correctly.

Some of the additional functionality provided by NETSCOUT's packet flow switches includes:

- **Aggregation:** Provide a central point for monitoring that can be accessed by a variety of IT groups; i.e., network operations and security operations.
- **Speed conversions:** Enable communications between network elements and monitoring and security tools even when the elements and the tools support different access speeds.
- **Filtering:** Reduce the load on the monitoring and security tools by only delivering traffic to the appropriate tools.
- **Slicing:** Improve security by removing the payloads from packets so that tools only see the packet headers.
- **Replication:** Improve efficiency by simultaneously sending the same packets to all of the appropriate tools.
- **Stripping:** Support virtualization by either removing the headers created by virtualized solutions and sending the traffic to the appropriate tools or keeping the headers and using the information in the headers to create a detailed picture of the virtualized environment.
- **Load balancing:** Improve performance and extend the life of existing tools by load balancing traffic over multiple instances of the same type of monitoring or security tool.
- **De-duplication:** Reduce the load on the monitoring and security tools by dropping duplicate packets.

Use Case: Visibility at scale

Customer's environment

As discussed in this white paper, over the last several years the speed of Ethernet links has been steadily increasing. As a result, the vast majority of data centers have network segments running at a range of speeds; e.g., 1 Gbps, 10 Gbps, 40 Gbps and in some cases, 100 Gbps. The continually growing speed of Ethernet links creates issues that make providing visibility very difficult. One of those issues is the load that these high speed links deliver can tax the capacity of the company's performance and security monitoring tools. Another issue is that aggregating

[19] http://www.netscout.com/product/enterprise/switches-taps-2/

high-speed traffic streams, each of which is experiencing microbursts, results in traffic with very high traffic spikes.

It is common to have the customer deploy both security and performance monitoring systems and packet flow switches in multiple locations world-wide. Locations may be distributed regional sites and one or more centralized network operations centers (NOCs). Some tools are supported locally, such as passive security devices and packet capture appliances, while select traffic is copied and sent to the NOC(s) for centralized analysis by higher capacity tools.

The NETSCOUT solution

NETSCOUT provides line-rate performance and advanced packet processing capabilities in a compact form factor for distributed locations via its nGenius PFS 4200 appliances. For large data centers, customers often deploy an nGenius PFS 6010. A typical deployment scenario is presented in Figure 3, with nGenius PFS 4204s aggregating traffic from multiple locations and sending that traffic to the data center.

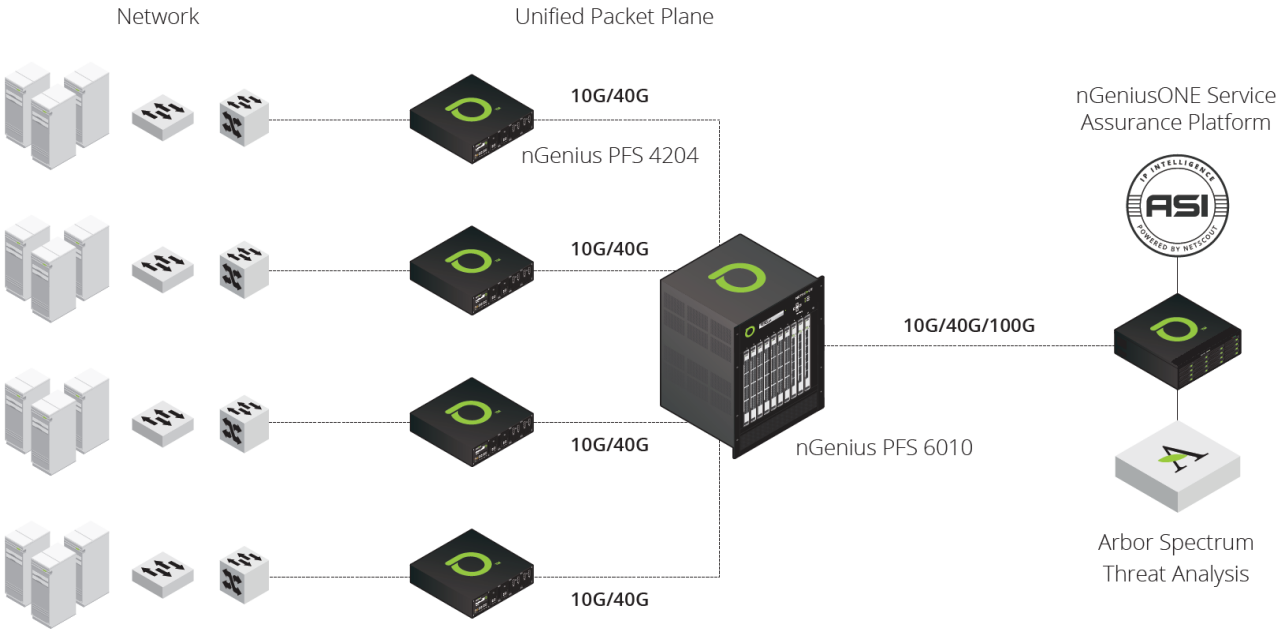

Figure 3: Visibility at Scale

Summary

During the last decade, the business infrastructure has become digital with increased interconnections among products, processes, and services. This movement on the part of companies of all sizes and types to become a digital business is causing companies to fuse together their business and IT strategies into a digital business strategy.

Because of the large and growing impact that a company's IT infrastructure has on it business

processes and overall profitability, an effective digital business strategy must focus equally on the key components of the IT infrastructure as well as on how to monitor the performance and security of the infrastructure. A company's data center is the most critical component of the company's IT infrastructure. Unfortunately, a number of technological trends are causing data centers to evolve dramatically and making the task of monitoring the performance and security of data centers significantly more difficult.

One result of the movement to adopt digital business initiatives combined with technological changes such as automation and virtualization is that network professionals will spend less time configuring devices and more time on proactive management tasks such as security and performance monitoring. In order to be successful, network organizations must architect and implement a visibility platform. The key characteristic of that visibility platform is that it must converge the current silos of visibility onto a unified packet plane.

Other characteristics of the required visibility platform are that it must:

- Scale to support continually higher speed links and a growing number of monitoring devices without losing any data.
- Have the capability to access packet level data at full line rate.
- Have the capability to fully analyze traffic in real-time and make appropriate decisions based on that analysis.

NETSCOUT's unified packet plane, built with its nGenius PFS purpose-built appliances, is an industry leading visibility platform. One of the key architectural principles of this approach is that it logically separates the network from the monitoring and/or security systems by employing a self-organizing mesh of nGenius packet flow switches. One of the many advantages is that it can monitor both the physical and virtual components of the infrastructure and it enables the network organization to make changes to the network without having those changes impact the monitoring and/or security systems. In order to overcome the well-documented latency and throughput challenges that can be associated with software-only solutions, another key architectural principle of NETSCOUT's approach is that some computationally intensive activities, such as processing encapsulated traffic and eliminating duplicated packets, are performed in dedicated hardware.