The Need for Active Visibility

// White Paper

Overview

The transition from an age of systems of record to an age of systems of engagement has led to profound changes in the way information is used in an organization. These changes have now become powerful market forces that are impacting the information technology landscape today. Consumerization of IT has led to new types of mobile devices being used to access critical information in an enterprise. As a result, there has been a rise in deployment of off-prem applications (whether cloud-based or hosted externally), virtualized applications, and a desire by line of business owners to use Big Data analytics or cloud-based applications to gain competitive advantage. This confluence of events has added more layers of complexity, inhibiting visibility for enterprise IT administrators and changed the span of control of traditional IT organizations irreversibly.

One of the tenets of IT service delivery is 24x7 operational excellence. In a consumer-led era, issues of service downtime, poor application performance and security risks are business debilitating. Put simply, you cannot manage what you cannot see.

This white paper spells out a new way to gain visibility into IT management and address key areas that are top of mind for a CIO and other IT leaders today: increase IT effectiveness in the areas of security and compliance, application/network performance management (APM/NPM), customer experience management (CEM), and data integrity.

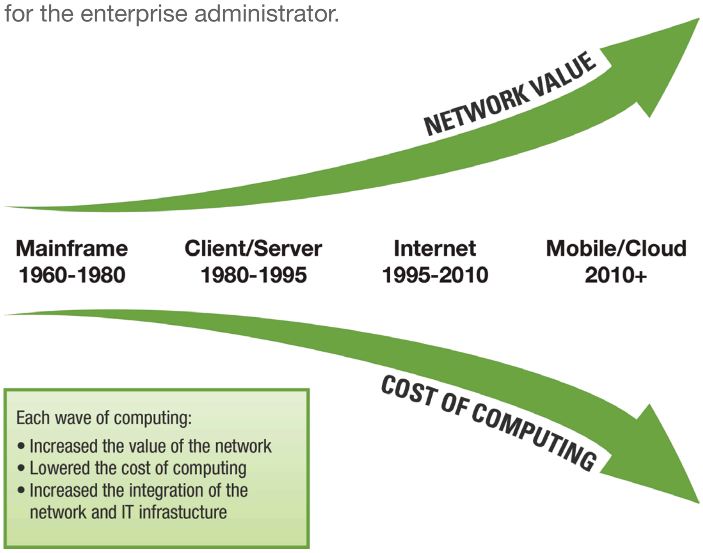
> Live traffic feeds are increasingly being used by the modern enterprise to gain visibility for security and operations management

IT Transformation: You Cannot Manage What You Cannot See

Consider the following findings from a recent survey done by ZK Research:

- 90% of mean time to resolution is in identifying the problem
- 75% of problems are first identified by end users, not by the IT department
- 83% of companies' network budgets is used to "keep the lights on"

These are unflattering statistics that scream for a different methodology to manage the transition. Over the last few decades, the drop in cost of computing has coincided with the corresponding increase in the value of the network. Today, the network has become an integral part of the IT infrastructure and there has been a rapid rise in the deployment of network traffic-based analytic systems (sometimes referred to as "tools infrastructure"). As traffic is the real truth, operational analysis systems invariably rely on real-time traffic feeds from the network to provide just-in-time insight for the enterprise administrator.



Each wave of computing:
- Increased the value of the network
- Lowered the cost of computing
- Increased the integration of the network and IT infrastucture

Figure 1: Network value and the falling cost of computing over the last few decades

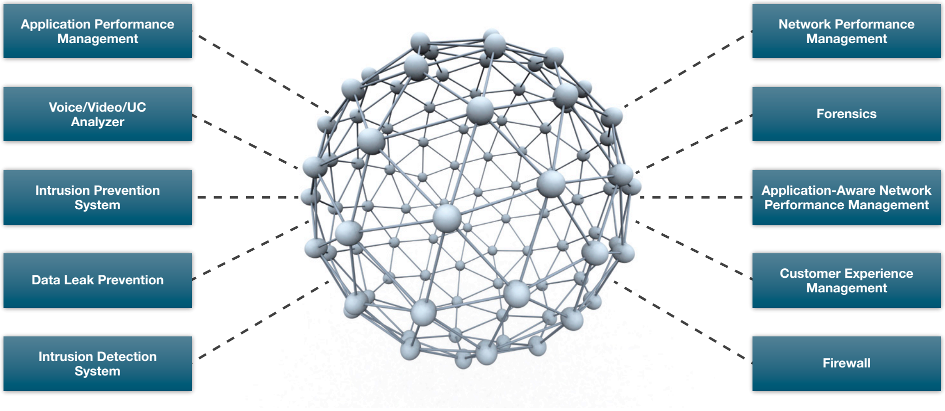

Application Performance Management
Voice/Video/UC Analyzer
Intrusion Prevention System
Data Leak Prevention
Intrusion Detection System
Network Performance Management
Forensics
Application-Aware Network Performance Management
Customer Experience Management
Firewall

Figure 2: Increasing use of traffic-based tools to manage IT

Need for Change: How Status Quo Bogs Down An Enterprise

The model of directly connecting traffic-based operational systems/appliances to a network has led to several bottlenecks for many reasons. This legacy method of connecting such operational systems directly to the network is no longer sustainable for the modern, agile enterprise for the following reasons:

1. Semantics without performance means more exposure: Although network speeds have increased rapidly to support compute and application needs, the processing power of security and other operational analysis systems that rely on traffic has not kept pace. The network has rich performance but poor semantics, while such security/operational tools are rich in semantics but poor in performance. For this reason, a network upgrade from 10Gb to 40Gb could make upgrades to operational systems extremely expensive and yet not provide the necessary performance to prevent business exposure.

2. Continued proliferation of IT operational tools: Legacy IT management methods deploy more operational tools every time a network is upgraded or expanded. This is unsustainable, extremely expensive, and directly limits the scope of visibility, impacting IT effectiveness in the process. A more prudent way would be to modernize infrastructure while consolidating operational tools, thereby offsetting the need to add more/new operational tooling every time a network is expanded or upgraded.

3. Relevant traffic, not just more traffic: To cope with these issues, there is more specialization today in these analysis systems than before. New systems often focus on highly-specialized types of analysis that require access to certain types of traffic and not all network traffic. For example, there is no need to deliver non-voice traffic to a voice analyzer. A customer experience management system on the other hand would need to correlate specific transactions to different IT systems for maximal effectiveness.

4. Technology obsolescence: Historically, the network has not been very adaptable to changes. As new paradigms for network virtualization and software-defined data centers take hold in the enterprise, logical abstractions and new encapsulations will be created that are not readily interpreted by existing operational tools.

5. Serial vs. parallel evaluation of new technologies: Enterprises often have a need to evaluate new technologies to be proactive against threats and outages, putting a great deal of strain on IT's time and responsibilities. This challenge calls for the need to parallelize such technology evaluation so that initiatives can be completed faster with a higher return on investment.

6. "Take Back the Night" (and the weekend!): When changes need to be made to the type of traffic being analyzed, they result in changes being made to the production network. Change control windows are typically at odd hours in the night or the weekend. In addition to slowing business agility, it puts different teams with different mandates (e.g. network team and security team) on an unnecessary collision course.

The result: a decrease in relevant data delivered to specialized tools leading to a rise in blind spots, a reactive operations/security management, lengthened project cycles, stressed operational staff and a suboptimal return in investment for the IT organization. Modern enterprises can do much better with a new approach!

Active Visibility to Meet Business Needs: A New Approach

A new approach needs to be taken to address the aforementioned challenges. Active Visibility refers to secure, intelligent, and pervasive use of traffic-based visibility in real time to instantaneously meet dynamic business needs. Intelligence here means providing just the relevant traffic that a specialized appliance/analytics application/tool needs, instead of delivering a traffic fire hose to the latter. The ability to select and deliver customized traffic streams to each operational system greatly reduces the processing overhead of the assigned systems, allowing for peak performance by those systems. Pervasive refers to the ability to provide traffic views regardless of location—at the interface to the WAN, in the core of a data center, inside a server, between servers, before/after an application delivery controller (ADC)/security appliance, or even in a remote site such as a branch office. This traffic-based visibility approach ensures that analytics applications and other operational tools get just the requisite data in real time, allowing for a proactive rather than reactive approach. The rest of this white paper articulates how this approach accelerates an organization's ability to meet its business needs.

Active Visibility refers to secure, intelligent, and pervasive use of traffic-based visibility in real time to instantaneously meet dynamic business needs

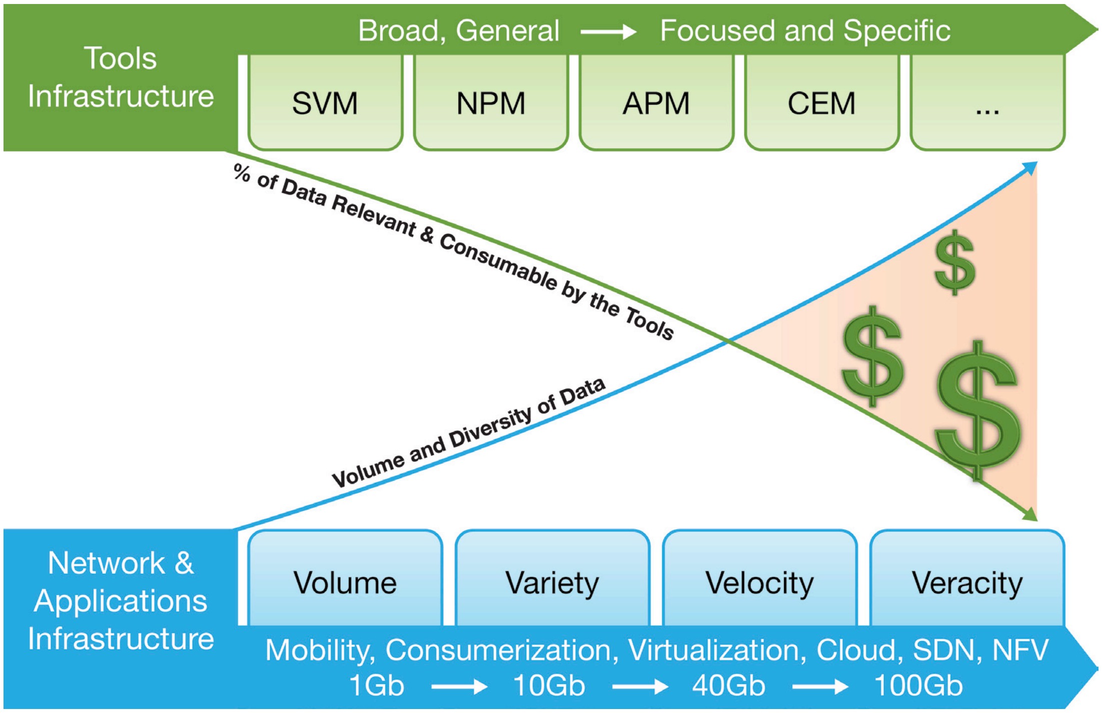

Tools
Infrastructure
Broad, General → Focused and Specific
SVM
NPM
APM
CEM
...
% of Data Relevant & Consumable by the Tools
Volume and Diversity of Data
$
$
$
Network &
Applications
Infrastructure
Volume
Variety
Velocity
Veracity
Mobility, Consumerization, Virtualization, Cloud, SDN, NFV
1Gb → 10Gb → 40Gb → 100Gb

Figure 3: Choke points to effective IT management are resulting from overload caused by irrelevant data

Security: You Are Only As Secure As Your Weakest Link

Organizations today operate in a landscape of dynamic threats where the security solution is no longer single-tiered. A unified threat management approach involves a multi-tiered security solution that requires multiple/bundled security appliances/tools to deal with these threats. Such a solution includes Web application firewalls, malware detection, intrusion detection/prevention, data loss prevention, and many more. As all these security devices need to inspect various components of network traffic in real time, an efficient way to distribute relevant network traffic to these security devices becomes essential. When deploying an inline security solution, multiple security appliances may have to be serially chained for comprehensive and scalable security; administrators should also protect against failure of any single device becoming a single point of failure for the entire network. Administrators also need to schedule maintenance upgrades on the inline security appliance so that they do not impact the production network. All these goals can be accomplished by using an Active Visibility solution for security, while concurrently offering the ability to consolidate other operational tool deployments. As shown in Figure 4, the Active Visibility solution pre-processes the traffic to intelligently distribute the traffic to different security appliances used in the infrastructure. Without the use of such a visibility solution, if the security system is only receiving a portion of the data (say 80%), your enterprise has an exposure to what it is not seeing (20% in the example). Your security strategy is only as strong as its weakest link.

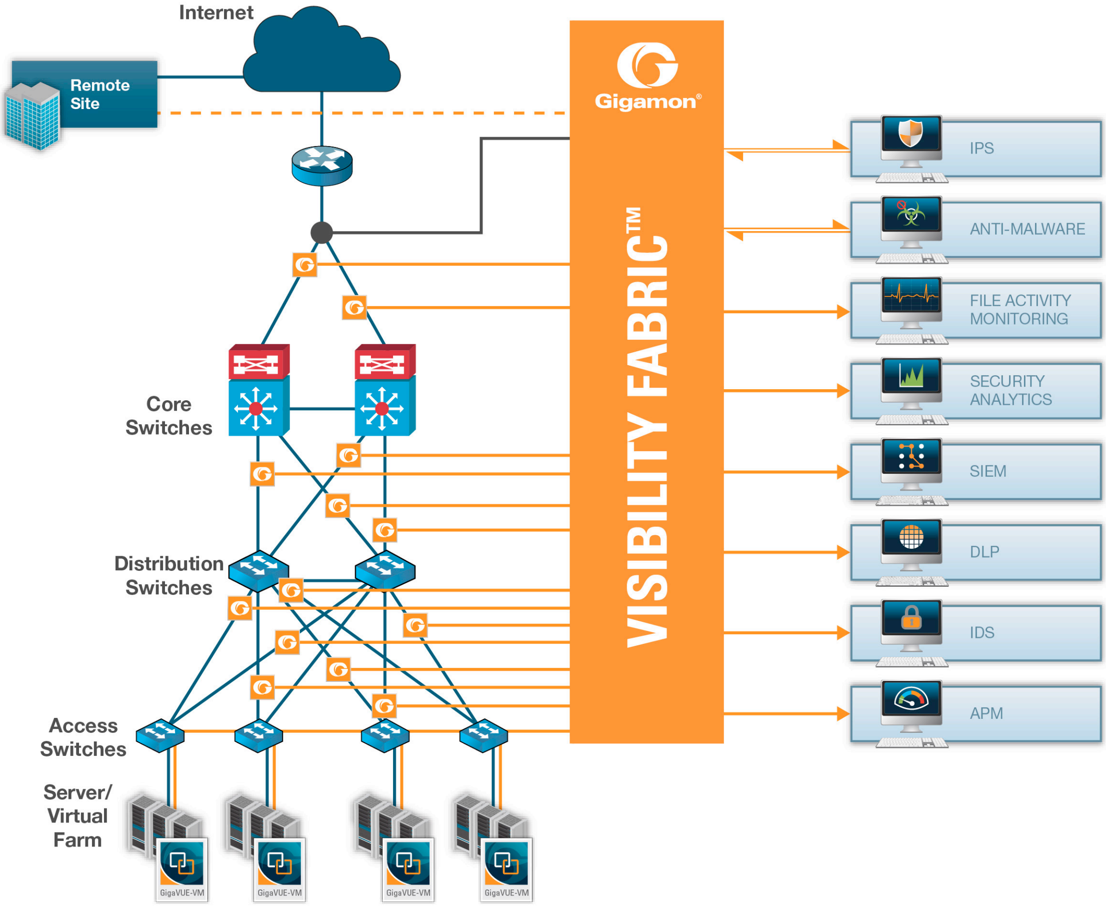


Figure 4: Active Visibility with the Visibility Fabric consolidates access to traffic for operational systems and security devices by providing pervasive, intelligent visibility to traffic from any location in the enterprise

Network and Application Troubleshooting: Shorten the Mean Time to Innocence

Poor application performance often leads a user to first ask "Is the network down?" The network team therefore has to ensure "Mean Time to Innocence" in addition to maximizing infrastructure uptime. Network performance management tools can rarely handle the peak load of the network, causing them to be overrun, without appropriate pre-processing of traffic fed to the network performance management tool. In order to be proactive, network performance management systems with packet capture capabilities should be efficiently deployed by connecting them to an Active Visibility solution. Examples of pre-processing done by such a visibility solution include packet slicing, de-duplication of identical duplicate packets from different monitoring points that might arrive in a time interval, offloading overloaded network devices from NetFlow data generation, etc. Empower your organizational staff to be proactive by having the tools to diagnose your entire network, not just select locations.

Customer Experience Management: Maximize Your Customer's Experience to Minimize Churn

Customer experience is a key success factor for many businesses. Web-based businesses, e.g. e-tailers, Web portals, app stores, Web sites that handle tablet/wearable/device registration must pay special attention to customer experience, as its absence leads to dissatisfied customers and customer churn.
The effectiveness and performance of a customer experience management tool can be maximized by pre-processing traffic in an Active Visibility solution before it is delivered to the customer experience management tool. Examples of such pre-processing include traffic slicing, filtering out irrelevant traffic, time stamping closest to transaction source for accurate latency tracking, eliminating duplicate packets resulting from monitoring multiple points in the IT infrastructure, and many more.

Compliance and Data Integrity: Minimize the Organization's Exposure

Data integrity has become harder to ensure today because of the advent of virtualization and emerging paradigms such as network virtualization or software-defined networking (SDN). Virtualization has led to distributed applications in a data center, leading to more east-west traffic in a data center. Transactions that were previously handled by a single host may now be split across multiple hosts in a data center or distributed between an on-prem host and a host located at a different location or a cloud provider. For accurate monitoring of application performance, more visibility is required into the various interactions between hosts. These interactions can lead to more traffic duplicates as switched network packets are captured from different locations in the network. An Active Visibility solution can eliminate such duplicates before they are delivered to the tools. In addition, the use of new network virtualization or other SDN paradigms within a data center to create logical networks means that important data could be hidden behind new encapsulations that the operational tools cannot decode. Content-based filtering in an Active Visibility solution allows important data to be detected and extracted by the visibility solution before it is delivered to the target tools.

Summary

This white paper described a modern method for gaining Active Visibility into an enterprise's technology infrastructure to meet its business needs such as security, customer experience management, compliance, and data integrity. By relying on the ultimate truth—traffic in real-time—Active Visibility delivers the benefits of real-time, pervasive, intelligent access and insight into traffic flowing through an enterprise infrastructure.

Gigamon has pioneered a new approach where the characteristics of this Active Visibility approach are delivered through a solution called the Visibility Fabric. Over 70 of the top Fortune 100 enterprises have discovered the benefits of Active Visibility with Gigamon's Visibility Fabric. Your organization could similarly benefit; find out more details at
http://www.gigamon.com/visibility-fabric-architecture