

Why 10Gb/s Networking Changes Everything



As a CIO or senior IT executive it's typically your responsibility to ensure your organisation's critical business systems are available, scalable, reliable and, of course, secure. A key component of your role is to ensure that your organisation stays compliant with a barrage of regulations covering everything from PCI to FISMA and RegNMS. Because of increasing network speeds, complexity and loads, the strategies that have been employed historically to guarantee the integrity of your critical systems are now no longer technically or economically sustainable. A failure to address this fundamental issue has the potential to put both your brand and your compliance status on the line.

This overview explains why the future of network monitoring and security looks very different to today's appliance-centric world and why forward-thinking organisations are deploying next-generation, distributed monitoring and recording fabrics. If you're planning an upgrade to 10Gb/s anywhere in your network, or you're planning to refresh any of your appliance-based network monitoring or security systems in the next 12 months, then, as a company officer you have a responsibility to read on.

As the speed of networks increase, the tools used to monitor, protect and manage them must work harder to keep up with the increased throughput. The trouble is that in many instances they simply can't keep up. There's a very good technical reason for this and it's because the underlying architecture that many of today's systems use to capture

packets from your network (for the purpose of analysing them to work out what's happening) is based on standard network interface hardware that was never designed to cope with 1Gb/s networks, let alone 10Gb/s. It's what's known in the networking industry as 'packet capture's inconvenient truth' and it typically starts to impact the performance and integrity of systems as they hit 2Gb/s. Of course, there are exceptions, and every vendor makes promises about the 'exceptional' throughput capabilities of their specific systems, but from our experience the truth is often far removed from the marketing hype. As a senior decision maker it's your job to ask the difficult questions of your current and future vendors.

THE EFFECT OF DROPPED PACKETS

Understanding the impact of missed or dropped packets on today's monitoring and security tools is important, since the effects are often invisible to the untrained eye. An easy way to think of it is like a metal detector at an airport that 'skips' one in five people when the queue hits a certain length. Using this analogy, it's easy to see why the consequences of dropped packets can be extremely serious. For instance, if you're responsible for protecting critical infrastructure against cyber attack (think Stuxnet) and your monitoring infrastructure misses the vital packets that signal an attack, then you're exposed to a security risk.

Likewise, if you're responsible for ensuring your organisation



is compliant with PCI or HIPPA requirements and your security systems miss packets, then you're exposed to the risk of non-compliance. The consequences of a serious breach of network security or non-compliance with regulatory requirements can be extremely serious – impacting brand reputation, financial stability and, in the most serious cases, lives. You only have to look to the media for very recent public examples of monitoring and security breaches that have publicly exposed some of the largest companies and organisations in the world.

To move beyond 'tick-in-the-box' compliance and build an efficient monitoring and security infrastructure that enables you to identify significant events, and provide proof and evidence of any wrong doing, you have to deploy a fabric of systems that guarantees to capture every single packet.

THE NEED FOR 100% RELIABLE MONITORING AND RECORDING

To be of any value, it's essential every monitoring or security system that relies on captured network traffic sees a 100% accurate feed of data all of the time. In the words of a very senior IT executive at a major investment bank in London, "If you haven't got all the data then any analysis that you do is pointless." The problem is, the faster the network goes, the harder it is to capture 100% of the packets reliably.

The mass-adoption of new, network-intensive technologies – cloud-computing, VoIP, Skype, Facebook, etc – has caused per-user bandwidth requirements within organisations to explode, while simultaneously making organisations ever more reliant on the stability and security of their enterprise data networks for business continuity. As network dependency has increased, so too has the demand for accurate tools to measure, monitor and protect those networks.

The range of tools organisations considered 'critical' to ensure the integrity of the network now includes everything from VoIP quality of experience measurement (QoE) and latency monitoring to intrusion detection (IDS), data loss prevention (DLP) and sophisticated forensic analysis tools

that allow end-user behaviour to be reconstructed in the course of investigating anomalous network events.

In today's world, each of these monitoring tools manifests itself as a physical ('point solution') appliance that has to be deployed into already over-stretched data centres. In a world where hardware consolidation and application virtualisation are widely accepted as industry best practice, the continued proliferation of vertically integrated 'point-solutions' in the monitoring and security space is an anachronism. Moreover, in an environment where networks are increasingly geographically distributed, point solutions represent a costly, inflexible and hard-to-manage solution to the monitoring problem.

In addition to the issues of deployment and management, system inaccuracy and hardware over-load, there are operational issues associated with 'point solutions', too. Because packet-loss affects each point solution differently, when it comes to actually trying to work out how a particular event has impacted a business overall, the impact of not having a single, accurate source of traffic makes things very difficult very quickly.

Understanding what has happened during a network anomaly event generally requires input from more than one system. Given what we now know about these systems, there's a good chance that each system will have seen the event through a subtly different lens – recording different information that cannot easily be cross-matched across systems. And each system may have missed packets that are critical to accurately analysing the anomaly.

In combination, the lack of integration between point solutions and their tendency to drop packets under load makes it almost impossible for anyone to construct a truly accurate picture of what really happened. In reality, most forensic investigations into network anomalies stop on the day that they start because the detailed information necessary to build a clear and accurate picture of what actually took place simply does not exist or cannot be correlated across disparate systems.

These issues, which are faced by any organisations as they



make the transition to 10Gb/s networking, are serious and are only going to get more serious as users become more mobile and the network edge disappears completely. It's also important to bear in mind the world isn't going to stop at 10Gb/s; 40Gb/s and 100Gb/s networks are already being deployed and will be commonplace inside the next 10 years. A simple graphing exercise looking at bandwidth use over time extrapolated out over the next five years suggests that many, if not most, Fortune 500 organisations will break through the 10Gb/s threshold in their core network environments over that period. So these issues affect everyone and they need to be discussed. What's interesting however is that there are many vendors in the network security and monitoring industry that would rather not discuss them, for reasons that should now be obvious.

THE CASE FOR A MONITORING AND RECORDING FABRIC

The concept of a 'monitoring and recording fabric' is relatively new for most enterprises, but it has existed amongst government intelligence communities and large financial institutions for a number of years.

The basic premise is straightforward. It is now widely accepted that accurate, high-speed monitoring and recording is something that can only be delivered using purpose-built hardware, and not using systems that rely on standard network interface hardware (NIC cards).

By separating the monitoring and recording component of a monitoring solution from the software applications that interpret and analyse captured packets, a more robust, modular and scalable monitoring architecture can be defined. It's a simple textbook lesson in specialisation. Let the companies that specialise in monitoring and recording provide the monitoring and recording component, and let the companies that make great software applications innovate in the application space.

Based on our years of experience working with government security agencies, telcos and financial organisations, we've recognised the most important requirement for these organisations is the power to see every packet that traverses

their networks – capturing it, analysing it and, if necessary, archiving it for later deep analysis.

This capability requires a range of different systems that can be deployed at the edge of the network or at the core; systems that can reliably capture 100% of traffic on all the various segments of a network regardless of that segment's type or speed or traffic types.

To address this need, we've spent 10 years developing a range of open, flexible monitoring and recording systems that can be woven together into a 'fabric' that can genuinely deliver the 'power to see all' regardless of whether the network is using OC-3 connections or 100Gb/s Ethernet.



ENDACE MONITORING AND RECORDING SYSTEMS

At the core of an Endace monitoring and recording fabric are right-sized, purpose-built Endace Systems that can be deployed network-wide (from the edge to the core) and connected to the network using passive network taps that allow the network to be monitored without adding load. These systems capture a 100% accurate copy of every packet from the wire and make captured traffic available to multiple applications running in virtual containers hosted on the various systems that make up the fabric. Depending on the specific needs of a given network segment, systems may capture and store packets locally in disk storage or just analyse them 'on the fly'. Should longer-term packet storage



be a requirement then Endace Systems that support fibre channel can be deployed to enable packets to be offloaded to a SAN.

All Endace Systems can be centrally managed by a SOC or NOC team, thanks to our Linux-based Operating System software layer (OSm) that sits between the monitoring and recording hardware and the applications that run on top of it.

Where high levels of timing accuracy are required (for latency monitoring applications, for example) systems can be accurately synchronised (to nanosecond level) using a range of highly accurate timing inputs (such as GPS) to ensure all packets traversing the network can be accurately timestamped and tracked wherever they travel – even on networks that are globally distributed.

At the application level, Endace Systems are designed to run multiple applications simultaneously, each able to access the same common source of 100% accurate captured traffic.

This open and flexible virtual application environment allows organisations to choose the tools that they prefer to use – whether they're custom 'in-house' applications designed for a specific purpose, open-source tools, or commercially available monitoring applications – as opposed to being limited to a proprietary application running on a single-function point solution appliance.

CORE VALUE OUT OF THE BOX

To ensure Endace Systems deliver immediate out-of-the-box value a number of common best-of-breed tools have been integrated into Endace OSm. These tools – known collectively as the Endace Application Suite – come as standard on every Endace System. The suite provides solutions to the common core monitoring and security needs faced by every organisation, and includes:

- A high-performance, SNORT®-based, intrusion detection system that delivers the very highest level of network-wide visibility into the potential threats facing a network
- An industry-leading network analytics package proving rich

graphical views of the traffic traversing the network, and facilitating rapid drill down into raw packets for forensic analysis

- A Netflow Generator that provides any number of systems with a feed of 100% accurate sampled or unsampled Netflow feeds
- An application that enables packets to be rapidly extracted by users and/or routed to other systems on the network that require a clean feed of captured network traffic.



APPLICATION AGILITY

Endace Systems also provide a virtual hosting environment called Endace Application Dock, which enables third-party applications to be run on the host system. Depending upon system configuration, up to six applications can run simultaneously on a single system. Application Dock gives organisations the power to work with the applications that are most relevant now, not the applications that were relevant two years ago when the last refresh was done. We see it as the democratisation of the monitoring and security market place, and in our opinion, it's long overdue.

Endace has also launched a formal partnership programme to provide testing of software applications in the Application Dock environment. This programme is open to any third-party software vendor or Endace customer that would like to have its applications formally performance tested, benchmarked and certified as Application Dock compliant.



HORSES FOR COURSES

Every network is subtly different and every CIO or senior IT executive sees the world through a slightly different lens. Regardless of the differences, there is an evolving set of 'best-practice' principles for operating a solid reliable network that are common to every organisation, whether it is a government intelligence organisation, a trading company, a major telco, or a Fortune 500 multi-national corporation.

For absolute confidence, organisations need:

- A complete set of tools that delivers deep visibility into every aspect of the traffic running on their network
- The ability to deliver a 100% accurate stream of captured network traffic to every monitoring or analysis application that needs it
- A clear technology path that will enable them to move to 10Gb/s, and from 10Gb/s to 40Gb/s and beyond without having to rip-and-replace their monitoring infrastructure
- The ability to deploy new network monitoring and analysis applications quickly as and when their needs evolve and dictate. Ideally this would not necessitate a further investment in hardware with all the additional ongoing costs of management and deployment that would accompany that investment
- To reduce demand on already over-stretched resources such as data centre rack space and people.

By now, the benefits of adopting an integrated monitoring and recording fabric versus deploying a swag of point solutions should be obvious.

With a well-architected monitoring and recording fabric deployed, organisations are, for the first time, able to fulfil all of the requirements listed above, without the limitations inherent in adopting multiple, single-function point solutions. With a monitoring and recording fabric approach:

- Every application receiving traffic captured by the fabric is able to access a single, common and 100% accurate feed of filtered packets. This dramatically improves application performance and accuracy and reduces mean-time-to-resolution for network issues

- The need for data centre rack space is immediately reduced
- Organisations can work with their tools of choice rather than being stuck with the vertically integrated proprietary applications that come with point solution appliances
- New applications can be deployed as needs evolve and dictate
- Applications running across a fabric can be tightly integrated – enabling inter-application messaging, automated workflows and accurate alerting – dramatically reducing the risk of missed threats or anomalies and speeding mean-time-to-resolution for network issues
- A single, homogenous monitoring and recording infrastructure reduces management and deployment complexity and reduces demands on already overloaded SOC and NOC teams.

AN ARCHITECTURE FOR THE FUTURE

A new 'best practice' approach is required that meets the challenges of networking at 10Gb/s and beyond. That approach already exists – it's called a packet-capture fabric, and we've been helping our customers to deploy this next-generation architecture on some of the most powerful and complex networks on the planet.

So, whether you're making the 10Gb/s transition now, or refreshing any kind of 'point solution', a monitoring and recording fabric should be part of your consideration set.

Talk to us. We're more than happy to give you the benefit of our experience.

For more information on Endace products visit: endace.com
For enquiries email: enquiries@endace.com