NDR And NPMD: Their Role In Managing The "New Norm"

A Broadband-Testing White Paper

First published February 2021 (V1.0)

Published by Broadband-Testing

E-mail : info@broadband-testing.co.uk
Internet : HTTP://www.broadband-testing.co.uk

TABLE OF CONTENTS

BROADBAND-TESTING

Broadband-Testing is an independent testing operation, based in Europe. Broadband-Testing interacts directly with the vendor, media, analyst, consultancy and investment communities equally and is therefore in a unique space within IT.

Testing covers all aspects of a product/service from business rationalisation in the first instance to every element – from speed of deployment and ease of use/management, through to performance and accuracy.

Testing itself takes many forms, from providing due diligence for potential investors through to public domain test reports.

Broadband-Testing is completely vendor neutral and independent. If a product does what it says on the tin, then we say so. If it doesn't, we don't tell the world it does what it cannot do… The testing is wholly complementary to analyst-related reports; think of it as analysts getting their hands dirty by actually testing what's on the latest hype curve to make sure it delivers on its claims and potential.

Broadband-Testing operates an **Approvals** scheme which prioritises products to be short-listed for purchase by end-users, based on their successful approval, and thereby short-cutting the evaluation process.

Output from the testing, including detailed research reports, articles and white papers on the latest IT technologies, are made available free of charge on our web site at HTTP://www.broadband-testing.co.uk

EXECUTIVE SUMMARY

- A combination of changing trends in networking architectures and the impact of the pandemic is morphing the shape of networking infrastructures into more complex, distributed topologies.
- Working from home (WFH) has become prevalent and will not revert entirely back to the centralised office-based/hub and spoke form that has been in place for decades before, regardless of the pandemic receding and the resulting fallout.
- This means that a different approach is required to serving and security the user base – one that needs specific tools and a reorganisation of IT in order to successfully optimise the user experience while protecting them from cyberthreats.
- Gartner has observed that NetOps and SecOps teams need to work together in a tighter, more organised fashion and that tools such as NDR (Network Detection and Response) and NPMD (Network Performance Monitoring and Diagnostics) are the best solution for the next wave of IT.
- As with all IT solutions, not all NDR and NPMD tools are created equal; they need to intelligently monitor network behaviour patterns and allow proactive countering of potential threats, rather than simply responding when it is already too late. They also need to be quick and simple to deploy, yet flexible enough to cover all business requirements and the continuing change in the shape of networks.

WHAT EXACTLY IS A "RETURN TO NORMAL"?

2020 was the year of the "new norm".

This pandemic-led, revised state of play involved a huge shift to working from home (WFH) with a dissolution of centralised office working and a very different user management scenario as a result. The user base was no longer largely in one or more self-contained areas, but spread across broad areas, each with different variations on a theme at the endpoint; Internet connection type and speed, working hours, requirements, knowledge base… This, in turn, resulted in increased security risks, performance management issues, support issues; after all, the end game was to maintain the existing user experience (from being central-office based) as much as possible.

2021 is no different. And nor will 2022 be. This "new norm" really is – by and large – here to stay. Far better to be backing a service provider than a commercial real estate investor right now! Businesses are already embracing the very different, but often more efficient, cost fabric associated with deploying and supporting a WFH workforce and waving goodbye to expensive office space. But that fundamental change in the physical shape of IT and the underlying network infrastructure creates its own potential problems. Let's face it, even in a traditional head office-based infrastructure, or a classic hub and spoke, HQ and branch office topology, few businesses really knew exactly what was running across those connections, whether applications or other forms of data.

Visibility IS everything. How can you secure an element of the network if you can't see it? How can you optimise a data stream that isn't on your management radar? Simple answer – you can't. Do you actually need to? Absolutely. In its recent market guide for Network Performance Monitoring and Diagnostics (NPMD), Gartner noted that data monitoring and analysis is becoming increasingly difficult because of these infrastructure changes, with cloud-native architectures replacing the classic designs and thereby rendering simple NetOps and SecOps monitoring collaborations meaning "job done" as being a thing of the past. The hardly anticipated mega shift to WFH strategies over the past year has simply complicated matters even further.

The Changing Shape of Networks

During the first UK lockdowns as a result of the COVID-19 pandemic in 2020, the shift to homeworking became mainstream news, not simply an IT-related topic, with reports on company employees forced to work from home questioning as to why they ever had to go into the office in the first place. The opportunity to effectively reset the "norm" in the workplace concept – no commuting and more flexibility with time - has been widely embraced. It has resulted in changes in data/Internet usage patterns however; peak traffic was occurring at very different times of day to those observed historically.

But then, the one constant in the world of IT, ironically enough, happens to be the primary variable – change. Constants are easy to manage – where they exist – but variables are anything but. Hence, why "adds and changes" are regularly referred to as an IT managers' worst nightmare. At any time, managing those adds and changes is challenging, but the past 12 months has witnessed an ever-changing global landscape, married to what was already a radically changing IT landscape, thanks to cloud adoption and significant advances within a company's IT infrastructure as job roles move around and "power" changes hands – IT roles are morphing and changing. Over the past two decades, IT in general has seen a change in mindset, from technology-driven thinking to a solutions-based approach and this is being reflected within the infrastructure itself. The emerging NetOps and SecOps tie-ins that Gartner has highlighted show how autonomy for certain aspects of IT is equally being consolidated, not least as a result of the quest for "agile IT" and the unavoidable digital transformation of a business.

As a result, the contemporary network footprint looks very different to what it did 10 years ago for sure, or even five years ago. Change is, indeed, the new "constant".

One specific point Gartner made was the need to "Increase alignment between network operations and security operations, by coordinating NPMD procurement decisions with security analytics solutions, including network traffic analytics tools." Additionally, the guide talked about the goals of NetOps and SecOps being more tightly aligned, given that they both rely on capturing and manipulating network traffic data. Therefore, combining resources in a single entity means relying on job-specific tools, notably NDR (Network Detection and Response) solutions.

The advice was to future-proof network monitoring by investing in network performance monitoring and diagnostics tools that provide the required level of visibility in hybrid environments, including edge network and cloud network monitoring.

Substantiating this thought, Gartner states that "by 2024, 50% of network operations teams will be required to re-architect their network monitoring stack, due to the impact of hybrid networking." Taken literally, that is an enormous re-investment in tools, education and mindset. Moreover, businesses cannot wait until 2024, they need to act right now, such is the speed of change and impact thereof. So, what are the basics in terms of the aforementioned NPMD and NDR tools that are required in order to manage these fundamental infrastructure changes?

A SOLUTION FOR MANAGING CHANGE: NDR AND NPMD

Whatever the changes over the decades in IT, network infrastructures and the ever-increasing security threat, preserving or improving the user experience has rightly remained paramount.

And another constant is finding and using the right tools for the job. In the current networking landscape, two of those key tools identified for managing, securing and optimizing the network and end-user service delivery are NDR and NPMD. Starting with the former, NDR is used to detect and prevent malicious network activity, investigate and perform forensics to determine root cause, and then respond and mitigate. It does this by initially providing greater visibility into what is actually happening on the network, using ML (Machine Learning) and AI (artificial Intelligence) software technology to identify unusual behavioural patterns for example which, in turn, enable security teams to identify and block any suspicious network activity, thereby minimising the impact.

Moving onto NPMD, these products are generally considered to be tools that take in and manipulate a number of different data sources – for example, network-device-generated health metrics and events; flow-based data sources and application-level traffic. Note, not all NPMD tools support all of these areas – some are still simple, raw packet-based data capture products which simply are not up to the task of resolving contemporary network issues. Fundamental to a modern-day solution is the ability to provide insight into the quality of the end-user experience, based on network-derived performance data. What has changed out of all recognition in recent years is what is considered to be that "network". Before it was simply a collection of LAN or WAN based network devices, servers and endpoints.

Now the focus has to be on the same single view of the "network" but this will be across on-premise, Data Centre, SDN, cloud and hybrid environments. And, as more of the workforce continues to operate long-term from the home or other remote locations, so this expansion of the network continues. This means the need to remotely manage and optimise user experience for performance, security, application availability and reduce the MTTR (Mean Time To Repair) problems becomes paramount. Remote users tend to be nervous and distrusting of technology – thereby providing a guaranteed level of support and service delivery can help enormously with their productivity.

Providing that level of service delivery is also essential in a multi-tenant environment, such as where a Service Provider is delivering a range of services to many different customers from a single management point. Being able to customise that offering, while still operating from a single management point is essential, both for quality-of-service delivery on the one hand and economies of scale for the Service Provider on the other.

Switching back to NDR, one of the primary issues created by this expanding WFH network is that, from a security perspective, the attack surface has therefore expanded too. This coupled with the endless rise of increasingly complex and sophisticated threats, that are capable of bypassing existing perimeter and endpoint protection, means that the mindset has to change from "protected" to being proactive towards potential threats with a detect and respond mentality. This is why NDR tools, as highlighted by the aforementioned Gartner guide, have become a fundamental component of a company's defensive armoury. It is all about allowing SecOps to detect risks in their infancy – ones that bypass traditional cyber security approaches - and respond accordingly, even where traffic is encrypted. Part of this new view of the network is the ability to detect potential issues with previously ignored east-west traffic within the network; a network, remember that now spans from BYOD and IoT devices to cloud connectivity. In so doing, a company can equally protect against malware and non-malware threats, including insider attacks, credential abuse, lateral movement, and data theft.

Another much documented area where both NPMD and NDR are instrumental to successful threat defence is that of zero-day (unknown threat) attacks - malicious code that has not been identified before. They exploit vulnerabilities as advanced persistent threats or targeted attacks, purposely designed to penetrate network defences, being beyond the detection of classic, signature-based detection devices such as AV or IDS/IPS. Instead, the only way to counter such attacks is by using technology that finds indicators of compromise (IoC), rather than attempting (and failing) to block these threats. Not only does the behavioural analysis approach detect potentially malicious zero-day threats, but it also enables response and forensic analysis – this is the key element in being proactive.

What cannot be over-emphasised, especially when managing a workforce that is spread across the globe potentially, with many individual workers, is the speed of response to potential threats. Being a remote site does not prevent an attack from spreading and causing chaos across an entire network, however virtual and dispersed that network is. Key to this is simplicity – centralised management, easy status visibility, courtesy of a customised management dashboard, reducing the time to value. Options such as a library of pre-defined dashboards help here, so a company can be up and running with a tailored NDR/NPMD solution within minutes, that is actively analysing the network for potential threats. It also minimises the required skillsets and training, in order to use the solution to its maximum potential. Preset examples include monitoring of videoconferencing services, streaming services, utilisation of VPN, monitoring of SaaS services such as Office 365 and social networks, as well as omnipresent protocols such as DNS and DHCP.

When a preset is applied, all the underlying features, such as profiles, report channels, widgets and dashboards are automatically set up and enabled, so it really is a one-click operation – the essence of time to value. Dashboards can be optimised to suit the role of the user – for example, whether from a NetOps or SecOps background. It means that, regardless of the skillsets and knowledge bases, the NetOps and SecOps teams can integrate using the same platform – fundamental to Gartner's guidelines.

It also means relevant, real-time information is always to hand, whether status reports on infrastructure or application delivery, or identifying the number of ongoing security incidents, including their severity. Importantly, templates are not set in stone, but are periodically updated, based on adds and changes, such as new cloud services, new application protocols or even just to reflect changing trends in user preferences.

Tied in directly with the data and application monitoring and analysis is the reporting capability, key being to provide complete visibility to every element of the system, regardless of the information source. Earlier it was noted that roles within IT and networking are changing; the C-level influence is greater than ever. Board members want accountability and they need to see it – flexible reporting capabilities provide that visibility.

IN CONCLUSION

The shift in workforce locations and related network infrastructure changes – cloud, hybrid, remote, WFH – is forcing companies to forever change the way they manage and secure that user base.

Gartner has identified that, in order to succeed in this absolute requirement, NetOps and SecOps teams need to work closely together, rather than in isolation, or simply on a casual interaction basis, and this means bringing specific tools to the fore. NDR and NPMD have been cited as the perfect solution to this potential crisis point in networking and IT change.

It is important, however, to understand that – as in any other aspect of IT – NDR and NPMD solutions are not all equal in terms of their capabilities and fit; in some ways – for example, flow versus packet-based – they can even be radically different. Aspects such as being able to intelligently monitor network behaviour patterns and allow proactive countering of potential threats, while still being quick and simple to deploy and manage, are important considerations to factor into the decision-making process.

One decision that doesn't need to be made, it seems, is that you do need these tools. If in doubt, just ask Gartner…