Publication date:
April 2024
Author:
Roy Illsley

Deep Packet Inspection In The Cloud Era

Why This Technology Should Be Part Of Your Network Monitoring Armory

Brought to you by Informa Tech

Omdia commissioned research, sponsored by Riverbed

Contents

Summary

Catalyst

Operational network monitoring is generally known as network visibility. On an enterprise network, this means an organization is capable of monitoring, capturing (as needed), identifying, and analyzing network traffic as flows into, across, and out of its network environment. Growing use of non-traditional network environments, such as cloud computing environments, remote or employee home networks where bring your own (BYO) computer is common, or operational technology (OT) environments, means organizations need to reconsider their approach to network visibility and need new approaches to performing deep packet inspection.

Omdia View

Network administrators use network monitoring systems to identify device or connection failures, or issues such as traffic bottlenecks. There is no standard definition of the term “network monitoring.” However, the generally accepted definition is “the provision of information that network administrators need to determine, in real-time, whether a network is running optimally.” Omdia classifies network monitoring into three categories:

- **Network packet analyzers:** these examine the data in each packet moving through the network to determine if they are being routed correctly, if employees are browsing prohibited websites, or if sensitive data is being removed from the network.
- **Application and services monitoring**: these identify which applications are being used by which business units within an organization and maintain network integrity to ensure the applications and services operate within acceptable limits.
- **Access management monitoring**: these ensure that intruders are not given access to network resources.

Traditionally, obtaining this packet-level visibility meant using taps, or SPANs on the physical network at key locations. However, as software environments and working practices have changed, access to the physical network via the use of taps has been restricted or made unavailable. This has left the network operations team with gaps, or blind spots, in its ability to monitor the network traffic.

Omdia is seeing strong demand from customers to leverage network packet-level visibility for various public cloud and SaaS use cases, such as making public workload migration faster and less

 © 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

risky, lowering cloud costs, meeting cloud compliance, monitoring the use of SaaS applications, and gaining visibility in the cloud-native container traffic.

The acceleration of cloud migrations continues to shine a light on the visibility gaps and blind spots that appear when organizations move workloads and applications to the cloud without a well-thought-out, holistic monitoring strategy. Network packet inspection is foundational to ensuring consistent and pervasive visibility across the entire hybrid environment and needs to be built in early into the cloud and SaaS migration process.

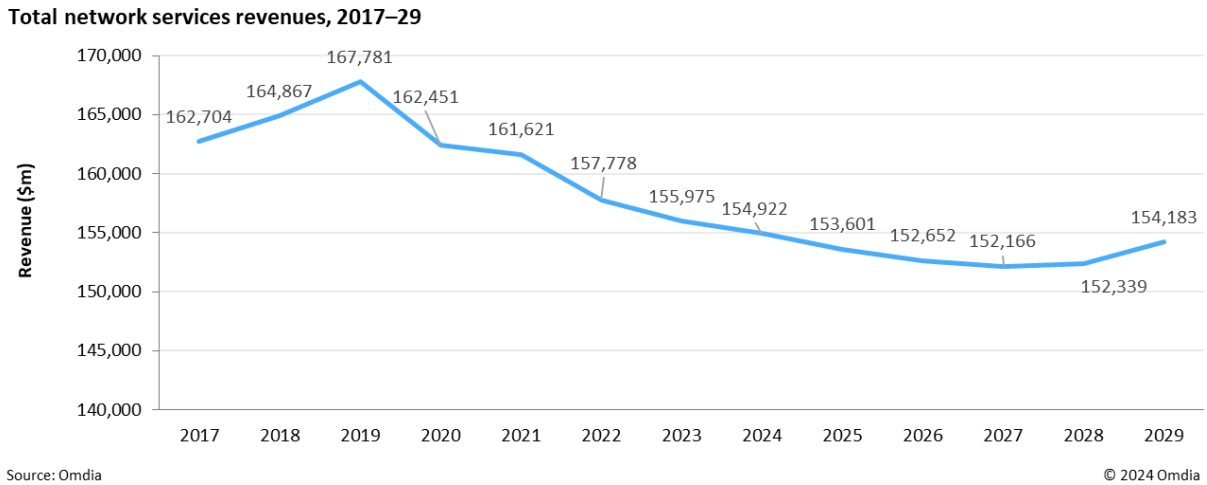
Key Messages

- The network services market will return to growth in 2028.
- Understanding the challenges of traditional deep packet inspection in a hybrid multi-cloud environment.
- A new approach to performing deep packet inspection is needed.

 © 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Market Data

Figure 1: Network Services forecast



Source Omdia

The enterprise network services market is shifting on the back of opposing forces and remains volatile (see **Figure 1**.) A product shortage in 2022 resulted in some projects being delayed to 2023. Although the supply chain disruption is easing, network vendors hint that the balance will likely return to normal closer to the end of the year. However, with a potential recession, pent-up demand is not likely to sustain growth through 2024. The network services market contracted more sharply than anticipated in 2022 due to the exchange rate impacts seen in multiple countries. With increasing interest rates and inflation just two of many uncertainties plaguing the world in 2023, many enterprises are laying off employees. Omdia expects more enterprises to take a cautionary approach, choosing to sweat assets rather than begin new projects in the near term.

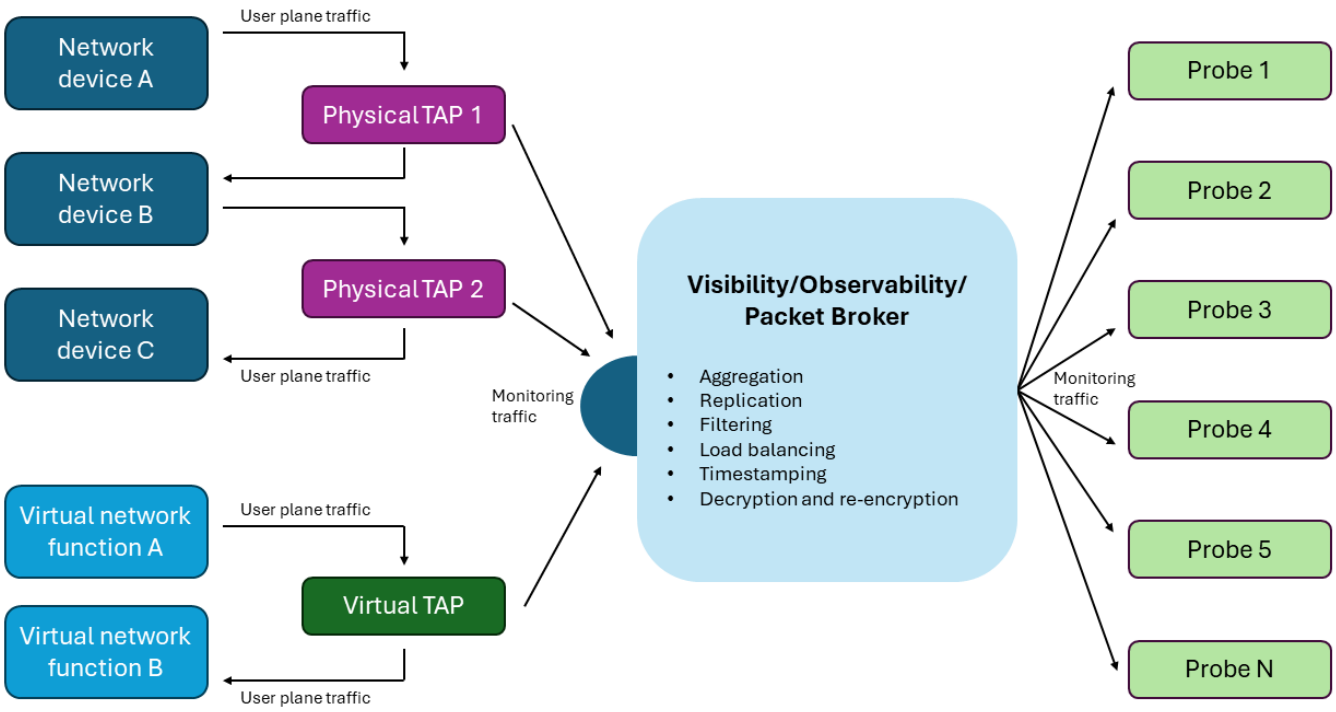
Global inflation was around 7.0% in 2023, according to the International Monetary Fund (IMF). While it may be down from a peak of 8.7% in 2022, it is still higher than the 4.7% seen in 2021. A price reset is likely to take place in the market as inflation drives up operation costs. Total enterprise network services revenue stood at $160bn in 2022 and is forecast to decline by a six-year CAGR of 0.6% to $154bn in 2028. The growth in managed network services will not be able to stem the contraction in core network services. The trend of enterprises migrating away from MPLS and private leased circuits (PLCs) to less expensive fixed broadband or dedicated internet access (DIA) with a managed security service wrap will continue. Some network migration projects may stall as new projects are postponed to conserve funds but are likely to resume as confidence in the market improves.

 © 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Challenges Of Deep Packet Inspection In Modern Organizations

Historically, network managers would use designated ports on a network appliance (e.g., a switch) to send a copy of network packets seen on one port (or an entire VLAN) to a monitoring tool where the packets could be analyzed. This technique was known as “port mirroring” or “switch port analyzer” (SPAN). **Figure 2** shows the traditional approach to deep packet inspection where if the utilization of the switch was high, it would drop SPAN packets; hence, this technique was only suitable for low-throughput spot-checking. A more robust solution involved network test access points (TAPs), which were physical devices that sat in a network segment between, a switch and a router, for example. The TAP makes a 100% full duplex copy of the network traffic without interfering with the performance of the production network devices (switches, routers, firewalls, etc.) and without impacting user plane throughput. The TAP then sends this network traffic copy to the network and/or security monitoring tool.

Figure 2: Traditional deep packet inspection



Source Omdia

 © 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

However, in the new environments such as cloud, cloud-native, SaaS, and hybrid working there has been a proliferation of endpoints, and the wider use of encryption has meant these traditional methods of accessing the network are being challenged.

Cloud computing uses the internet and is more vulnerable to a wider set of threats, such as lateral movement from one cloud service to an adjacent one. It is also unlikely that customers will be able to inject any additional hardware into the cloud service, and virtual TAPs may have restrictions placed on them by the cloud providers in terms of what data can be captured. It is also worth noting that the service provider market is different than the general enterprise market. In general, the scale of the network and the traffic carried is much greater by service providers. This can often lead to a lot of finger-pointing between network infrastructure suppliers as to where the root cause of a performance issue lies (what layer, which device, etc.). Adding to the complexity, the teams responsible for the operation of network monitoring and the analytics it feeds are often distinct. This can lead to more finger-pointing when packets go missing as to whether the monitoring or the analytics is to blame.

Cloud-native, which is mostly associated with the use of Kubernetes, is a far more complex environment than the VM-based environments it is replacing. In the cloud-native environment, the clusters consist of nodes, and the nodes consist of pods, and each pod can be one or more applications, so doing DPI means you need access at the pod level.

SaaS applications and the infrastructure they execute on can range from the ISV's own data centers to a mixture of public cloud and co-location facilities. The other consideration in SaaS environments is these applications may have been produced using proprietary technologies, and as such, network monitoring needs to extend beyond IP and TCP packet analysis to application data. The key message is that IT has no access to TAP the SaaS network.

Home or hybrid working involves the need to support endpoints potentially in any location. Some are not corporate owned or managed, and may be connected by any method, therefore the traditional approach does not work. Work-from-home traffic often bypasses the corporate network, going straight to SaaS applications, so traditional packet capture can't see it.

Encryption standards like transport layer security (TLS), IPSec, and secure shell (SSH) encrypt the packet payload, concealing critical data needed for visibility. Don't underestimate how TLS 1.3 wreaks havoc on network security architectures, particularly out-of-band decryption and delayed inspection approaches. This is arguably the top driver of decryption architecture reviews. As a result, organizations must understand the ramifications, and the differences from HTTPS, particularly when it comes to DPI.

 © 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

New Approaches To Deep Packet Inspection Are Needed For The Cloud Era

The evidence above clearly shows that physical network taps will not work in many cases, so a software solution must be developed. A software solution is advantageous in that it:

- Can be deployed on an endpoint (e.g. a personal device or server), enabling it to have visibility of encrypted traffic, SaaS applications, and work-from-home scenarios.
- Offers visibility into cloud-native environments such as Kubernetes, where traffic is dynamic and ephemeral.
- Captures additional data from the endpoints, which can be used to gain deeper insights into application and end user data.

However, a software approach must consider the operational aspects of managing a networking monitoring solution. Deploying the software to the identified locations should not be underestimated, as setting up a new software distribution process in organizations typically involves engaging and agreeing with multiple stakeholders, many of whom will not have any interest in DPI. Once the software distribution has been established, it must then be maintained and managed, which can become a resource-intensive task.

Riverbed has identified a simple yet effective approach to resolve the challenges of DPI in modern environments. Riverbed uses agents that are installed at the endpoints, meaning Riverbed does not have to decrypt any traffic to perform DPI. Because its agents operate at the endpoints pre/post the decryption point, it can access the traffic legitimately based on the terms of use of the software at the endpoint. Riverbed has reduced the software distribution challenge by building the agents into its existing customer experience software that already has distribution processes set up.

Riverbed's approach was to develop a unified agent that could capture user experience, network performance, application, or IT infrastructure-related information and to transport this information to a central data repository for further analysis. Using this approach, only the single agent requires distribution and management, reducing the resources required in the IT department to operate the solution. The different capabilities of the agent can be enabled by a simple remote software control process, which means customers can collect the information they require when they require it. This captured data is passed to NPM Plus where embedded AI is used to help with analysis. Omdia considers that NPM Plus is the equivalent of a level-3 expert on networking providing insights and advice to a company. By having access to DPI, organizations can use NPM Plus to accelerate root cause analysis, which could eventually lead to predictive maintenance.

 © 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Appendix

Author

Roy Illsley
Chief Analyst, Cloud and Data Center
askananalyst@omdia.com

 © 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

 © 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

 © 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.