Why visibility is key for NDR success

As businesses grapple with how to operate and thrive in today's unrecognisable landscape, cybersecurity is taking the top spot when it comes to organisational priorities due to escalating cyber-attacks.

According to Gartner, Network Detection and Response (NDR) tools delivered across on-prem, cloud and IoT are helping organisations to better detect suspicious activity compared to more traditional security tools.

It is therefore no surprise that we are now seeing rapid adoption of these tools by security teams to bridge the gap between SIEMs and endpoint detection and response tools, which facilitates enhanced threat hunting and protection against malware attacks and non-malware threats.

However, if NDR tools only have a partial view of network traffic, they can't effectively do their job. NDRs depend upon many sensors that are deployed to where the data flows from – data centres, internet access points, cloud, branch offices, retail stores – as they need visibility of all information in motion to detect, analyse and respond to threats. However, enabling this is not as straightforward as some security pros believe and must be considered when adopting any NDR solution to ensure that it delivers a full return on investment.

Clouded view

While companies are rushing to implement NDR tools to enhance their security posture, many don't consider that deploying them can present a series of challenges. It's no secret that networks have become increasingly complex – what with the surge in connected devices due to the pace of digitalisation and the prevalence of remote working – meaning visibility across their entirety isn't something you can take for granted. First off, east-west traffic is difficult to monitor: today's corporate networks are extremely spread out, made up of myriad devices and users and travelled by excessive volumes of data. This can only be analysed by deploying more and more sensors at the edge, which is problematic; or by one all-encompassing sensor, which would inevitably pick up irrelevant, duplicate traffic, creating inefficiency.

Another factor standing in the way of comprehensive visibility is traffic encryption: **the vast majority of north-south traffic and more than half of east-west traffic** are encrypted in order to protect it from prying eyes. That, of course, means it's also sheltered from monitoring tools themselves. While NDRs can make some sense of it by manually inspecting encrypted data, they are infinitely more effective when analysing decrypted traffic. We don't need to tell you that decryption is no walk in the park: it often requires the re-architecture of networks and data centres, and it's a costly affair as decrypting algorithms take a heavy toll on CPUs. This issue can represent a real obstacle to NDR optimisation.

A matter of time

It seems counterintuitive that a solution adopted to improve and simplify threat hunting can actually make it more of a challenge, without the right tools in place to optimise it. Far from being a plug-and-play solution, NDRs and their sensors are incredibly time consuming to deploy and maintain. All the housekeeping related to NDRs can end up taking InfoSec teams away from their job of detecting and responding to threats. A huge proportion of these professionals, after all, are experiencing overworking and burnout as a consequence of the pandemic, so the last thing they need is more admin on their plate to take away precious time from what really matters – keeping the network secure.

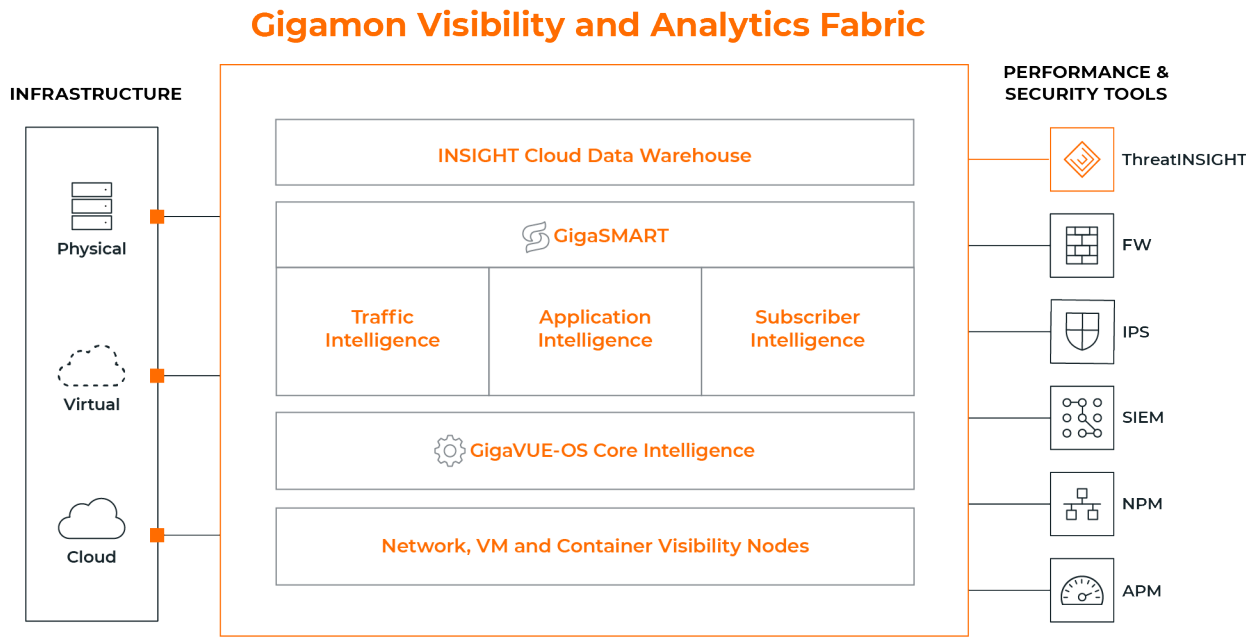
Why is NDR maintenance such a laborious task? Well, it's important to consider that IT infrastructure is constantly changing, adding complexity to the mix. Think of the transformative impact of COVID-19: workforces are largely based at home accessing the network via personal, unmanaged laptops, unsecured IoT devices are growing in numbers and hybrid cloud environments are gaining momentum. Furthermore, NDR sensors need to be constantly deployed and redeployed, meaning security teams are often unsure they have a clear view of the whole picture.

Breaking the bank

It's also crucial to bear in mind that NDRs are multi-million dollar per year solutions. Firstly, they represent a significant upfront investment. Secondly, storing and analysing such vast volumes of data is, of course, very costly and risks making the entire project too much for companies' balance sheets. While improving threat detection is an imperative in today's circumstances, it's clear that a piece of the puzzle, one that can maximise NDR investments, is missing.

How Gigamon can help

STRONGER SECURITY STARTS WITH NETWORK VISIBILITY



The Gigamon Visibility and Analytics Fabric collects data-in-transit across physical, virtual and cloud infrastructures and transforms it – optimising, decrypting, securing – before distributing to your tools.

An effective security posture requires seeing ALL traffic across your network — not just a portion. You need to know what the threats are, and how best to respond. Gigamon Visibility and Analytics Fabric sits between a business' infrastructure and its performance and security tools. It accelerates network detection and response with a cloud-native platform that delivers deep and pervasive visibility across the entire network, and provides insights for rapid threat hunting, investigation and forensics. It collects all information in motion across physical, virtual and cloud infrastructures, and then optimises, decrypts and secures it before distributing to your tools.

Gigamon Visibility and Analytics Fabric goes beyond any network packet broker to deliver a smarter, more proactive approach to network management, monitoring and security. It delivers optimised, full-fidelity data to security and performance monitoring tools, dramatically improving tool effectiveness and efficiency. High-velocity threat detection and response provides peace of mind, while advanced orchestration and automation enables your NetOps and InfoSec teams to do more, faster.

Once all information in motion has been discovered, it must be given context within the environment. As part of Gigamon Visibility and Analytics Fabric, Application Intelligence empowers IT teams and analytics tools with unrivalled application visibility and control by gathering clear, actionable and reliable data for efficient monitoring and security analytics. With App Visualisation, App Filtering and App Metadata, Application Intelligence provides unprecedented visibility into applications on the network, their behaviour and user experience.

UNVEIL ENCRYPTED TRAFFIC – COMPLIANTLY

The double-edged sword of encryption is no longer an issue: GigaSMART SSL/TLS Decryption creates centralised decryption, supporting tools all the way up to TLS 1.3. That being said, decrypting traffic, particularly when it encodes sensitive information about customers and employees, presents compliance issues and privacy becomes paramount. That's why a solution that allows organisations to enforce privacy rules can be an invaluable ally, particularly at a time when personal data, like patient records and bank information, is increasingly held online. With Gigamon, companies can ensure that only the tool processing specific traffic containing private information can see it; and can enable functions such as masking, where over-sensitive data is blocked from view. This way, Gigamon gets around the encryption problem by only showing traffic to the tools it matters to.

STREAMLINE NDR MAINTENANCE

Deploying sensors is not a once and done. That's why, as a SaaS-based service, Gigamon deploys and maintains all NDR sensors for you, meaning InfoSec and SecOps teams can focus on threat hunting and protecting the organisation. To streamline the monitoring of all traffic, Gigamon offers centralised visibility via a single location by accessing all east-west and north-south traffic. This way, sensors don't need to be deployed across multiple locations - offices, retail outlets and so on. With optimisation in mind, Gigamon only sends relevant, deduplicated and filtered traffic to NDRs, making their work far smoother and enabling lossless flow records. Finally, analysing all container traffic across public and private cloud instances can be incredibly difficult, but not for Gigamon, as it allows NDR tools to view and inspect all of these environments, turbo-charging efficiency.

We know obtaining pervasive visibility into your complex, ever-morphing network is a challenge. Gigamon manages these processes on your behalf, meaning you can hone in on valuable work, while ensuring nothing goes on across your network that you don't know about.

SPEND LESS AND SAVE MORE WITH NDRS

Investing millions in threat detection at a time when strong cybersecurity practices are imperative seems exactly the right thing to do. But that doesn't mean you shouldn't look at obtaining cost-savings in the process. By filtering, deduplicating and intelligently directing traffic to the right tools, Gigamon unlocks unparalleled ROI when it comes to NDRs.

Contact Gigamon today to learn how we can help you optimise your NDR investments.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com

12.20_01