IDC TECHNOLOGY SPOTLIGHT
Sponsored by: VIAVI Solutions

A "network" is characterized as an operational and security event horizon. But really, it is the resource that facilitates lines of business and enables creativity. Companies, contractors, and customers realize more benefits from a better network.

It's Not a Mystery — It's Your Network

January 2021

Written by: Christopher Kissel, Research Director, Security and Trust Products, and Mark Leary, Research Director, Network Analytics

---

Introduction

Despite best intentions, what gets emphasized about networks is the complexity of the job of cybersecurity professionals and operations in keeping the network up and running. From a scholastic standpoint, and somewhat salaciously, we talk about the adversary, various cybersecurity techniques, an expanding network surface, and network optimization. Forgotten are the reasons for networks. The network becomes a medium to transport data and deliver applications as well as a place to facilitate business. In short, industry analysts talk about the affectations of networking but not the power of the network.

This power shows itself across key business value measurements, including:

- **User productivity.** Networks that deliver a consistent and high-quality user experience boost user productivity. And bear in mind that the user can be an internal worker, an external partner, and an end customer (e.g., consumer in retail, patient in healthcare, client in financial services). Being able to closely observe and continually optimize network service levels allows the IT staff to always deliver the best possible user experience, boosting worker efficiency and effectiveness, partner interactions and importance, and customer satisfaction and spending.

AT A GLANCE

KEY STATS

- Roughly 44% of organizations expect security threats to be the biggest IT/security challenge they face over the next three years.
- 38% of organizations say the biggest IT/security challenge over the next three years will be modernizing and automating IT management.

WHAT'S IMPORTANT

- IDC expected digital transformation (DX) to be a driving force of business, but the effects of COVID-19 have accelerated this reality.
- Companies quickly deploying new architectures now require essential technologies to make up for the imposed technical debt.

- **Business agility.** Knowing the state of the network at any given moment heightens reaction times and service readiness when facing the ever-shifting demands of the digital era. In-depth network intelligence enables the use of precise thresholds, performance trends, and predictive modeling to full advantage when adding new sites, connections, users, Internet of Things (IoT) devices, shared resources, cloud services, data sets, and business applications to the network.

- **Cost savings.** Networks consist of many component parts, each with its own capabilities and constraints (and costs). Constant and detailed monitoring and analysis of the network ensure greater accuracy in assessing the operating condition of these components and drive properly timed upgrades or replacements. Timing is everything. Taking action too soon leads to overspending; taking action too late increases risk. Knowing exactly the demands on and status of network components at all times enables organizations to leverage digital solutions — both systems and services — for maximum efficiency and effectiveness.
- **Threat mitigation.** Industry metrics indicate that threats are often active within the IT infrastructure for months before discovery. And with data protection regulations tightening and worker/partner/customer sensitivities increasing, the ability to identify and mitigate threats early in the breach cycle delivers tangible benefits to business performance and perception. Comprehensive visibility and control enable the early identification of threatening traffic anomalies and help direct the proper security action required to eliminate the threat.

The right set of management capabilities makes the network more powerful and safer and enables IT organizations to deliver on the full promise of networking. This IDC Technology Spotlight discusses the best techniques to facilitate the smooth and secure operation of the network; the paper also covers the business value of a powerful, secure network.

The Big Picture

The best way to think of a network is as a technology that is trying to bring order to chaos. The on-premises network includes files, users and personas, mobile and stationary devices, ingress/egress ports, servers, routing tables, and any number of security devices. Axiomatically, these entities must work together flawlessly; otherwise, operational inefficiencies will occur (in the best case) or vulnerabilities that can be exploited (breaches) or severe performance bottlenecks may be introduced (in the worst case). The lead architect of an on-premises network creates an image of an NMAP, builds an LDAP for end users along with a hierarchy of identity controls, and then has an "ideal state" for rules, roles, and permissions for a working network and for reimaging. This is as hard to do as it sounds. However, for the sake of argument, let's say that the architect can stand up the network and set the dials to their liking. How successful will they be at any given time in the future?

Given the dynamism of today's network infrastructure, the answer is probably "partially successful at best." Even in a well-designed network, as many as 15–30% of all devices will be unmanaged. Any number of reasons lead to instability on the on-premises network. For example, devices may constantly drop off or enter the network, new software upgrades may not take hold, the network may reach capacity, routing tables may not update, or there may be physical changes in the network due to a power outage.

A monolithic, on-premises network construct is rapidly becoming an antiquated, almost naïve concept. The networks of today consist of public cloud access, direct-to-user applications, mobile access, and IoT devices, and one can make the argument that protection must be extended to social media as well. In other words, the network is truly "borderless." NetSecOps teams must gain visibility of a laterally expanding network surface without a clearly defined perimeter while shrinking the same surface to thwart the adversary.

Unfortunately, COVID-19 changes these rules further. Organizations dynamically reassessed their whole approach to networking — including technologies, techniques, tools, and talent. Work-from-home environments, new VPN structures, and a new call for virtual firewalls (or even connectivity without firewalls at all ingress/egress ports) change the paradigm of networking. The pandemic accelerates digital transformation for all organizations, and with this acceleration comes a more urgent call for a dynamic, stable, secure, automated, and adaptive network infrastructure. In networking, our next normal is nothing like the old normal; even the NetSecOps team is remote.

Let's simply understand that the next normal already exists and there is a real-life boogeyman on the other side of any given network (the adversary or adversaries), but let's also understand and appreciate two other points. The first is that the boogeyman is not unbeatable. The vintage rules about end-user and business-level hygiene, secure configurations, strong identity and access management, network segmentation, and layered defense still apply. Second, even in its imperfect state, the network is humming along and facilitating the line of business, bolstering communications, housing intellectual property, and implementing analytics to improve the custom experience. Common to both is applied network analytics that thwarts the adversary and creates resilience.

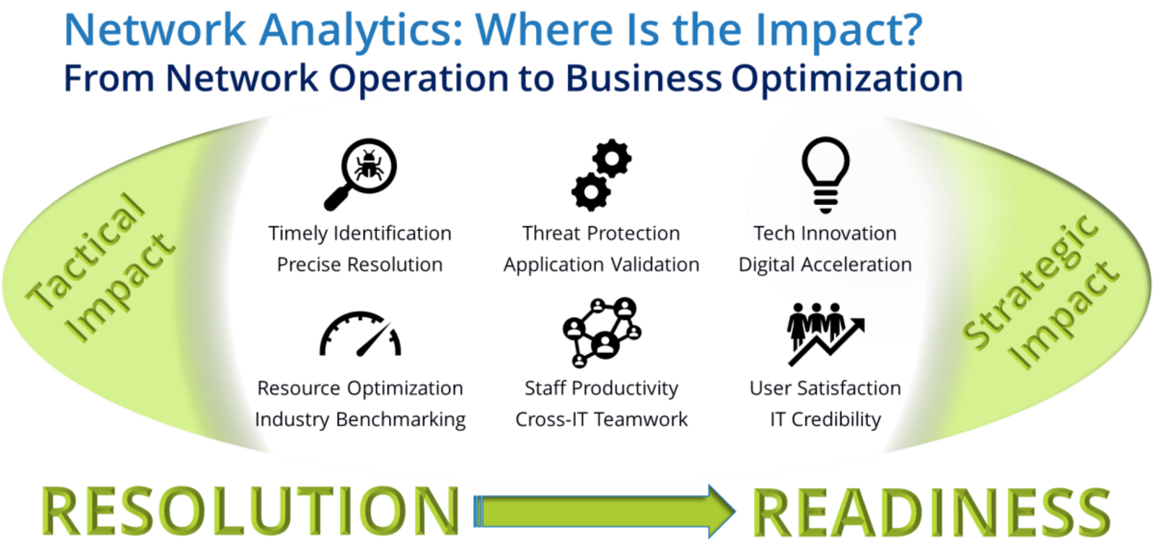
Bringing Out the Goodness in the Network

"Network analytics" is a fairly broad term, but the following characteristics define network analytics with some precision:

- **Data acquisition.** Digital information meets the network in bits and bytes. Data acquisition is the collection of data from devices, clouds, and appliances. The data acquisition cycle includes packet, log, flow, telemetry, and polling mechanisms that index data and establish timestamps.
- **Intelligent analysis.** Data ultimately has gravity. As data is collected, intelligent analysis can create baselines for network performance as well as user behavioral analytics (UBA) and heuristics, dynamically (or manually) establish thresholds for the detection of anomalies, and apply machine learning. Intelligence analytics can chain together events, target specific IT domains, and help reveal the root cause of a problem (i.e., security or a bottleneck in performance).
- **Management automation.** The problem facing IT teams in this analytics stack is that with each insight, there is a corresponding response. If these processes are always manual, even the best insights are of negligible value. Enter automation. A properly instrumented network can use insights to create workflows that correlate data on a single dashboard, develop context awareness for incident investigation, and point the team to a guided response; in so doing, it eliminates human error or misjudgment.

Network analytics has real power. Figure 1 illustrates the impact of properly applied analytics.

FIGURE 1: ***The Impact of Network Analytics***



Source: IDC, 2021

Figure 1 shows the transition from resolution to readiness as well as the desired impact or outcomes. But network analytics is also the diagnostic layer of the network. For instance, network optimization is not a trivial idea. As symptoms relate to sickness, so too does a poorly performing network lead to greater problems for the business. Examples include the following:

- **Latency.** Any number of network conditions can cause latency (e.g., a wrongly assigned server or routing table, connection to the wrong point of presence [POP], poor configurations), which can be problematic on all levels. If a consumer visits an ecommerce website, any latencies in that session reduce the chances that the person will make a purchase or return for future purchases. If an employee is experiencing latencies when working within a VPN, the temptation to use a workaround is too great to resist; once a workaround is adopted, the protocols that ensure a proper security posture are no longer effective.
- **Bandwidth.** Speaking of security, most security appliances are gated by capacity constraints. Security and information event management (SIEM) systems often have event per second (EPS) limits, and firewalls are expressed in Gbps. These appliances are reliable when under or at capacity. However, when burst traffic comes, or bad internal traffic handling occurs, the security appliances may drop packets and simply not work as well. As such the adversary often tries to create buffer overflow or accelerated conditions to overwhelm bandwidth constraints.
- **Applications.** Network performance is ultimately reflected in the applications. A network must have predictable performance for Office 365, Salesforce, and any number of independent software vendor (ISV) platforms to work. Even before workarounds are applied, workers are effectively stymied if applications become unavailable to them.
- **Resilience.** In addition to the management of alerts, alarms, automation, and workflow, network analytics provides a macro view. Network analytics not only can establish baselines for the present condition of the network but also can measure for drift over time. The network is forever taking snapshots of its state in real time; these associations, often referred to as a "golden state," can be a guideline when adding new devices or infrastructure. If there is a major impact event, network analytics can help with settings and reimaging in disaster recovery.

Considering VIAVI Solutions

VIAVI Solutions, located in San Jose, California, is a diverse $1 billion global provider of network test, monitoring, and assurance solutions for communications service providers, enterprises, network equipment manufacturers, government, and avionics. The VIAVI network analytics solution originates from the company's Enterprise and Cloud business unit.

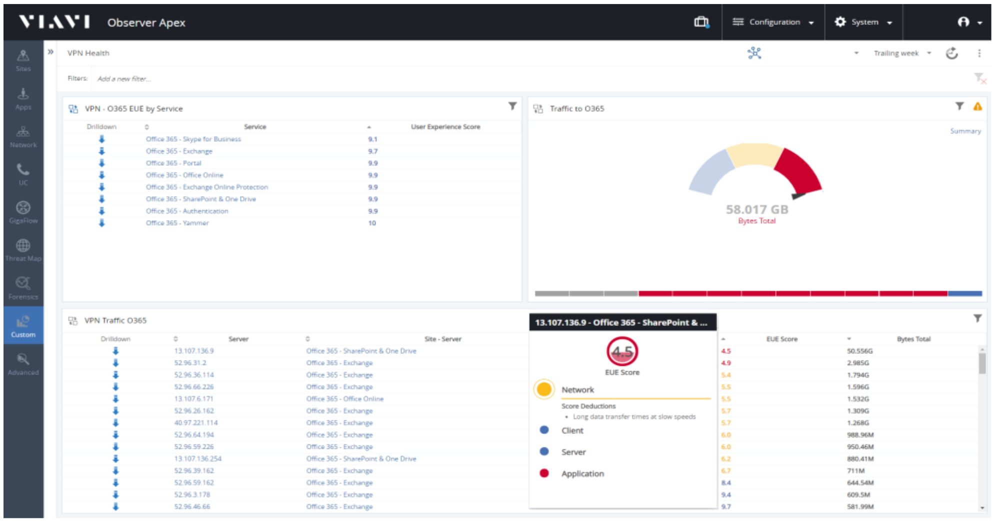
VIAVI Observer is a versatile network and security monitoring platform providing three major functions, each mapping closely to IDC's core network analytics functions: data collection, intelligent analysis, and command and control. The VIAVI Observer platform features high-performance packet capture, analysis, and storage, combined with enriched flow and active test data, to deliver high-fidelity network visibility. This allows enterprises to drive optimal service delivery without interruptions from network performance issues or security incidents.

> Network security impersonates the proverbial real estate agent when its mantra is "visibility, visibility, visibility."

Arguably, the central strength of Observer is its ability to track peer-to-peer sessions (conversations) and then frame the context into a holistic and evolving view of the network. The end-user experience score is a centralizing feature of Observer. Observer gathers inputs across the discrete elements of end-user exchanges — network, client, server, and application. For every network conversation, machine learning is applied and a color-coded single numeric value with problem domain breakout is assigned.

The network is dynamically mapped and explorable on dashboards. Visibility and telemetry include discovery of all servers, routers, appliances, and devices. More granularly, Observer establishes relationships among user-assigned IP addresses, MAC addresses, and usernames (see Figure 2). Additionally, the data collection and analytics are designed in such a way that there is not double TAP or double SPAN to refine the network.

FIGURE 2: ***Partner in a Box***



VPN Health

Filters: *Add a new filter...*

VPN - O365 EUE by Service

Drilldown	Service	User Experience Score
⬇	Office 365 - Skype for Business	9.1
⬇	Office 365 - Exchange	9.7
⬇	Office 365 - Portal	9.9
⬇	Office 365 - Office Online	9.9
⬇	Office 365 - Exchange Online Protection	9.9
⬇	Office 365 - SharePoint & One Drive	9.9
⬇	Office 365 - Authentication	9.9
⬇	Office 365 - Yammer	10

Traffic to O365

VPN Traffic O365

Drilldown	Server	Site - Server	EUE Score	Bytes Total
⬇	13.107.136.9	Office 365 - SharePoint & One Drive	4.5	50.556G
⬇	52.96.31.2	Office 365 - Exchange	4.9	2.985G
⬇	52.96.36.114	Office 365 - Exchange	5.4	1.794G
⬇	52.96.66.226	Office 365 - Exchange	5.5	1.596G
⬇	13.107.6.171	Office 365 - Office Online	5.5	1.532G
⬇	52.96.26.162	Office 365 - Exchange	5.7	1.309G
⬇	40.97.221.114	Office 365 - Exchange	5.7	1.268G
⬇	52.96.64.194	Office 365 - Exchange	6.0	988.96M
⬇	52.96.59.226	Office 365 - Exchange	6.0	950.46M
⬇	13.107.136.254	Office 365 - SharePoint & One Drive	6.2	880.41M
⬇	52.96.39.162	Office 365 - Exchange	6.7	711M
⬇	52.96.59.162	Office 365 - Exchange	8.4	644.54M
⬇	52.96.3.178	Office 365 - Exchange	9.4	609.5M
⬇	52.96.46.66	Office 365 - Exchange	9.7	581.99M

13.107.136.9 - Office 365 - SharePoint & ...

Score Deductions
- Long data transfer times at slow speeds

Source: VIAVI, 2021

NetSecOps vendors and the analysts who cover them speak about "speeds and feeds," and while that discussion is appropriate, we are still missing the mark.

The use case that VIAVI Observer is initially deployed to address may not be the only (or even the most important) target. For instance, Observer may be deployed to monitor the quality of VoIP phone calls, but in discovery, the SecOps team may find a server that acts as a DHCP server or exhibits C2C server connectivity behavior.

A tool like VIAVI Observer facilitates the desired goal of unifying IT and security workloads. IT and security objectives are not always aligned. A practical example is that a security team finds a Common Vulnerability Scoring System (CVSS) gap but then leaves it to the IT team to deploy the patch. Another example is that a security team suggests a new firewall policy but then requests that IT rewrite the permission when there is network availability.

The combination of IT and security teams strengthens the network as well. Security teams can identify lateral movement by entering a compromised user ID and seeing other affected systems. By stitching together user IDs, MAC addresses, and IP addresses, network teams can identify if a user is having trouble connecting to internal corporate applications. In addition, the quality of alerts that come from VIAVI Observer is such that the contextual awareness is gathered in one fell swoop. The end-user experience (EUE) score explains what hosts are affected and the severity of the alert. The fidelity of the score leads to the next logical processes that NetSecOps needs to follow to more efficiently and accurately rate and remediate the event.

Challenges

In the past few years, unifying processes that are traditionally IT management and cybersecurity has been paramount. The reasons for this are myriad.

- The lack of a common data set with customizable workflows and dashboards can be a detriment to cross-silo collaboration. A single interface for multiple teams can enable the automation of IT troubleshooting workflows and maximize business value of network infrastructure.
- The network surface is expanding and has become borderless. Hybrid architectures include public cloud, on-premises, mobile, IoT, and straight-to-use applications. It is almost impossible to place firewalls between all these surfaces much less allow the status quo of siloed IT and security approaches — there are too many gaps.
- There is a shortage in the availability of experienced people needed to protect networks. And yet, the show must go on; many security operations centers (SOCs) have generalists who are dedicated to both IT and security.
- Tool sprawl is a common problem. The best-of-breed approach to tools still exists; however, every time a new tool is introduced, so are different training and a new workflow.

VIAVI Solutions is competing with network performance monitoring platforms that offer security alerting and detection. The largest vendors in the SIEM, network security, and endpoint security segments are building XDR platforms and security frameworks designed to be holistic solutions. Meanwhile, many IT teams are seeking to develop streamlined workflows with automated response to network and service anomalies, improving the efficacy of existing tools. An opportunity for VIAVI Solutions would be that Observer might help an intrusion detection system (IDS) catch malware otherwise missed.

Conclusion

The various forms of cybersecurity defense all have merit — endpoint, data loss prevention, antivirus, web defense, and others have specific functions. Additionally, defenses used in combination create "defense in depth," and gathering telemetry from various data sources described in this paper also adds value in cybersecurity detection and response as well as network performance monitoring.

However, what VIAVI Solutions Observer does in quantifying the network actions of every device and user along with the quality of each transaction is an excellent vantage point for cybersecurity teams if the correct premise is that network status is the summation of conversations. While other cybersecurity technologies require context to understand the fidelity of an alert, Observer captures all relevant information in each session. Knowledge of all user sessions, if collected and analyzed properly, is a reliable indicator of a security compromise, which is the advantage that Observer provides.

About the Analysts

	Christopher Kissel, *Research Director, Security and Trust Products* Chris Kissel is responsible for cybersecurity technology analysis, emerging trends, and market share reporting. Mr. Kissel's primary research area is cybersecurity analytics, intelligence, response, and orchestration (AIRO). He also covers the processes that security operations center (SOC) analysts employ to monitor, detect, remediate, and mitigate threat actors attempting to attack a network within a security and vulnerability management and security analytics paradigm.
	Mark Leary, *Research Director, Network Analytics* Mark Leary is responsible for worldwide technology research and analysis focused on network management, including related analytics, AI/ML, automation, and programmability. Mr. Leary also examines advancements in enterprise and cloud network technologies; adoption of cloud services and software-defined systems; network management best practices; and the evolution of IT staff roles and skills in this demanding hyper-connected digital era.

MESSAGE FROM THE SPONSOR

VIAVI Observer Online Demo Video

To learn more about Observer Platform, please click on the link below for an online demo video. Using actual UI captures, watch how end-user-experience scoring can aid your IT teams in delivering optimal service levels. Should a problem arise, it also offers a simple method by which to quickly solve degraded user experience.

To watch the demo, visit ***https://www.viavisolutions.com/en-us/ptv/request-observer-demo***

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
5 Speen Street
Framingham, MA 01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com