VIAVI Solutions

How to Solve 6 of the Biggest IT Challenges in 2021

MANAGING NETWORK PERFORMANCE & CYBERSECURITY IN A SHIFTING LANDSCAPE

Contents

Introduction 3

CHAPTER 1
Problem Domain Isolation 7

CHAPTER 2
Cybersecurity Network Detection & Response 11

CHAPTER 3
Remote Working & VPN Management 16

CHAPTER 4
Network Capacity Planning 21

CHAPTER 5
SD-WAN Oversight & Posture 25

CHAPTER 6
New Deployment Rollouts 25

INTRODUCTION

Driven by a surge in remote access and increasing cost pressures, IT is amidst great upheaval that will impact how networks and applications are managed.

New or accelerated rollouts in VPN, SD-WAN, IoT, and cloud migrations among many others means IT teams responsible for network health and security must update tools, processes, and practices.

The cost of doing nothing and getting by with a patchwork of existing resources results in degraded service performance and increased security risk exposure.

What is needed are actionable insights into end-user experience and the supporting infrastructure. With this visibility, maintaining existing services is simplified and new applications can be deployed on time, within budget, and without negative impact to users.

Without comprehensive insights into both end-user experience and infrastructure devices, solving network performance and security issues becomes time and resource intensive.

In the case of security, reducing dwell time is critical — with the risk of intellectual property loss, regulatory fines, and compliance audits, **every second that a breach is left uncontained is money lost for the business**.

This e-book will examine some of the biggest challenges that IT teams now face and ways to solve them.

PROBLEM DOMAIN ISOLATION

Finding the root cause of service performance issues has always been challenging. Today's multi-cloud, vendor, and tier applications multiplies the difficulties to a whole new level.

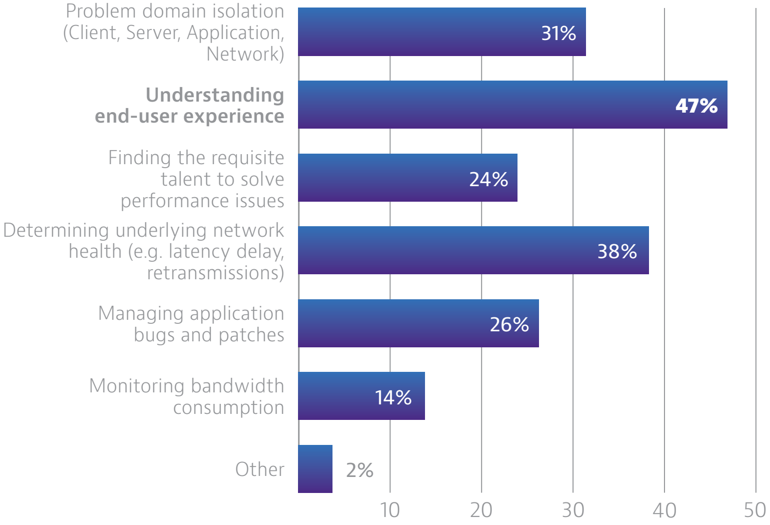
Not only does it take time to aggregate key performance indicators (KPIs) from different sources, but also the tools you have at your disposal can overwhelm you with too many or the wrong KPIs. This "KPI" overload is counterproductive and will misdirect efforts to solve the issue(s), or potentially leave you blind to ongoing performance problems

If isolating the problem domain down to client, server, network or application takes too long, it can be devastating for the business in lost revenue, productivity or even reputation.

DID YOU KNOW?

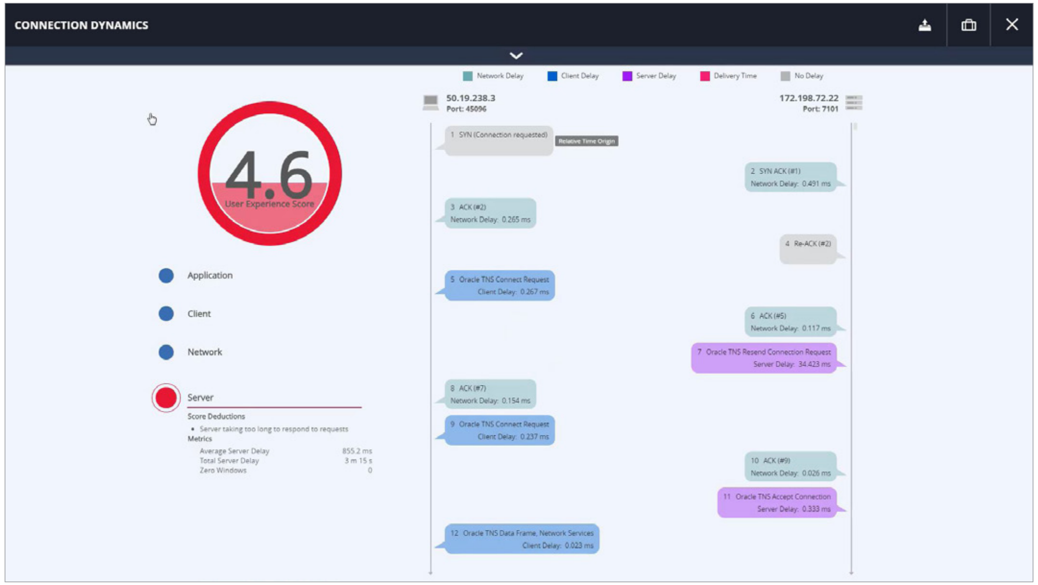
In the 2020 State of The Network Survey, 47% of IT professionals surveyed said that **understanding the end-user experience** is the top challenge for troubleshooting applications.

What are the top 2 challenges you face when troubleshooting applications?



Isolating Problem Domain for Network and Application performance using Observer

- **Monitor end-user experience** of every conversation with a single, numeric, color-coded score composed of 30 well-known and VIAVI developed KPIs
- **Pinpoint the source** of poor user experience whether caused by network, client, server or application
- **Visual troubleshooting** of multi-tier, multi-vendor applications
- **Conduct forensic deep dive** into individual client-server conversations
- **Validate that a real issue exists**, describe the impact (scope, severity, duration) and automatically pinpoint the domain.



Score Deductions

- Server taking too long to respond to requests

Metrics

Average Server Delay	855.2 ms
Total Server Delay	3 m 15 s
Zero Windows	0

50.19.238.3
Port: 45096

172.198.72.22
Port: 7101

1 SYN (Connection requested)

2 SYN ACK (#1)
Network Delay: 0.491 ms

3 ACK (#2)
Network Delay: 0.265 ms

4 Re-ACK (#2)

5 Oracle TNS Connect Request
Client Delay: 0.267 ms

6 ACK (#5)
Network Delay: 0.117 ms

7 Oracle TNS Resend Connection Request
Server Delay: 34.423 ms

8 ACK (#7)
Network Delay: 0.154 ms

9 Oracle TNS Connect Request
Client Delay: 0.237 ms

10 ACK (#9)
Network Delay: 0.026 ms

11 Oracle TNS Accept Connection
Server Delay: 0.333 ms

12 Oracle TNS Data Frame, Network Services
Client Delay: 0.023 ms

KEY TAKEAWAYS

1. End User Experience scoring can reduce **KPI overload and streamline root cause analysis**
2. Isolating problems quickly with visual troubleshooting and forensic deep dive leads to **reductions in mean time to repair**
3. **Minimizing downtime** means more satisfied end users and more time for IT to support business goals

CYBERSECURITY NETWORK DETECTION & RESPONSE

Today, security threats abound and repercussions have greater visibility and impacts. With remote access becoming the new norm, employees are using business devices for both professional and personal communications and may not be connected via VPN.

It is only a matter of time before a cybersecurity breach incident occurs. Between the loss of organizational intellectual property assets, substantial legal fees, regulatory fines, and reputational damage, the fallouts of a breach can be devastating to any business.

So how should you be more prepared?

According to EMA, enterprises who used wire data as a part of their normal cybersecurity toolset had shorter breach detection and response times and more confidence in workflows and processes.

This means **speedier containment** of the breach, **higher satisfaction** from operations teams, and **more time available** to focus on optimizing service delivery.

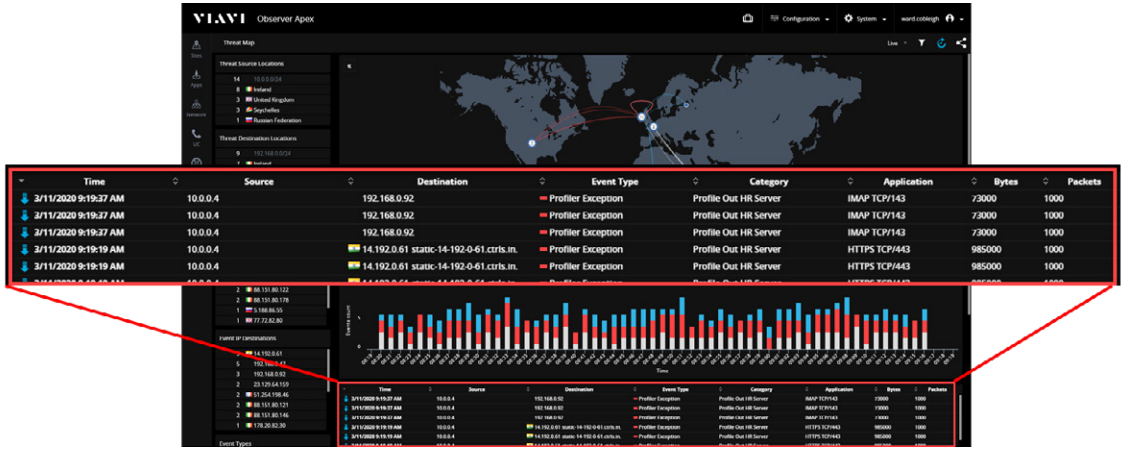
$3.86M
Global average total cost of a data breach in 2020

280 days
Average time to identify and contain a data breach

$1.0M
Average savings from containing a breach in less than 200 days

Source: 2020 IBM Cost of a Data Breach Report

6 Ways Observer helps to secure your cyber posture



Time	Source	Destination	Event Type	Category	Application	Bytes	Packets
3/11/2020 9:19:37 AM	10.0.0.4	192.168.0.92	Profiler Exception	Profile Out HR Server	IMAP TCP/143	73000	1000
3/11/2020 9:19:37 AM	10.0.0.4	192.168.0.92	Profiler Exception	Profile Out HR Server	IMAP TCP/143	73000	1000
3/11/2020 9:19:37 AM	10.0.0.4	192.168.0.92	Profiler Exception	Profile Out HR Server	IMAP TCP/143	73000	1000
3/11/2020 9:19:19 AM	10.0.0.4	14.192.0.61 static-14-192-0-61.ctrls.in.	Profiler Exception	Profile Out HR Server	HTTPS TCP/443	985000	1000
3/11/2020 9:19:19 AM	10.0.0.4	14.192.0.61 static-14-192-0-61.ctrls.in.	Profiler Exception	Profile Out HR Server	HTTPS TCP/443	985000	1000

- **Reduce dwell time** by identifying anomalous behavior and rogue activity with host and service profiling
- **Enter the MAC address** of a known compromised machine or username into the IP viewer to see where else the hacker could have gone
- **Detect lateral movement** by using SYN forensics in the integrated threat map or IP range scanning
- **Conduct back-in-time analysis** with packet capture and enriched flow to conduct evidence-based risk management
- **Document Distributed Denial of Service attacks** – if you see a spike in a certain type of service, captured wire data and flow provide the irrefutable truth about the attack
- **Leverage pre-configured and custom IP blacklists** to keep bad actors from accessing your networks.

KEY TAKEAWAYS

1. Detecting and identifying anomalous behavior with host and service profiling can **minimize the financial and reputational damage of a security breach**.

2. Comprehensive network visibility will help **identify, reduce and contain sensitive data** that is accessed o stolen by unauthorized users.

3. By documenting network transactions with forensic-level wire data that stands up in court, you can **minimize potential legal costs and regulatory fines** due to untimely reporting or lack of data.

REMOTE WORKING & VPN MANAGEMENT

VPNs have been implemented in organizations since IPSEC was defined in 1995 to help protect sensitive information — so they aren't new. But recent market changes that forced a dramatic increase in remote workers is a scenario networks were never designed to handle.

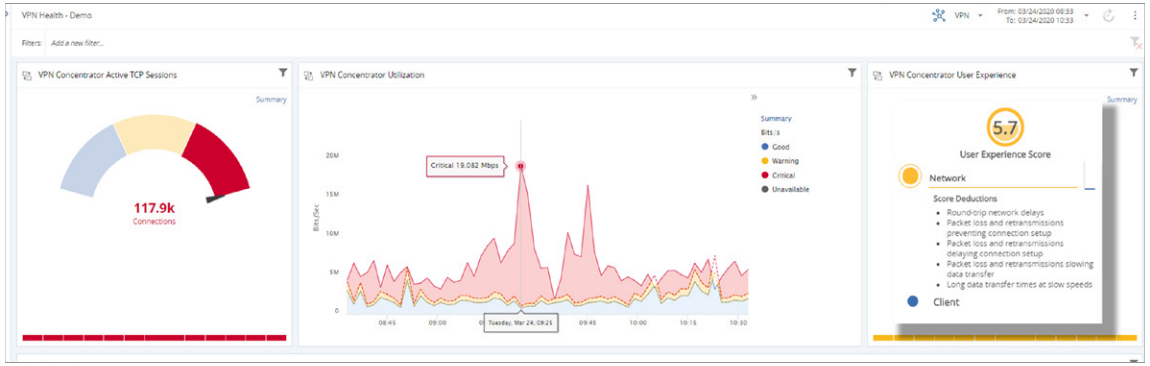
Not only are users remote but often, the engineers trying to troubleshoot are as well. Peak time traffic increases have caused access issues, slow application responses and conference call failures. The result? **Decreased productivity and lost revenue**.

> Teams have scrambled to rearchitect networks, implement split tunneling and other measures to counteract increased remote working, but are being hampered by network visibility challenges.

DID YOU KNOW?

According to research firm IDC, 6% of staff worked from home pre-COVID, 53% worked from home during the height of the pandemic, and roughly 30% will continue to work from home by 2021.

5 Steps for Managing VPNs and Remote Worker Access



VPN Health - Demo

VPN From: 03/24/2020 08:33 To: 03/24/2020 10:33

Filters: *Add a new filter...*

VPN Concentrator Active TCP Sessions

VPN Concentrator Utilization

VPN Concentrator User Experience

5.7 User Experience Score

Network

Score Deductions

- Round-trip network delays
- Packet loss and retransmissions preventing connection setup
- Packet loss and retransmissions delaying connection setup
- Packet loss and retransmissions slowing data transfer
- Long data transfer times at slow speeds

Client

- **Monitor VPN providers** to identify if they are the source of the problem
- **Monitor VPN concentrators** to understand VPN health and capacity
- **Monitor the remote users' experience** at a moments glance while also conducting a deeper dive into the forensic level data
- **Detect and respond** to bad actors in the network with an integrated threat map and IP viewer
- **Profile remote endpoints** to identify anomalous behavior that may indicate compromise

KEY TAKEAWAYS

1. Proactive VPN monitoring minimizes business downtime, shortens mean time to repair, and reduces support costs
2. Listening to your network will optimize the remote end-users' experience and increase employee productivity
3. Quickly pinpointing problem domain increases service desk tier 1 resolution rate

NETWORK CAPACITY PLANNING

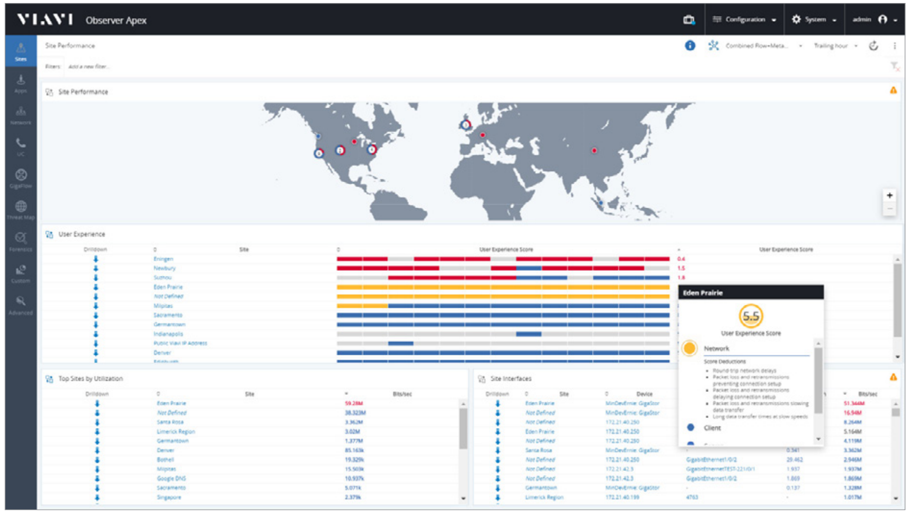
Capacity planning is an ongoing process that comes in many forms, from sizing requirements for a new project in a specific site, to optimizing current assets and resources, making hosting location go/no-go decisions, rolling out multi-tier applications, planning for acquisitions, or business growth and change.

There is a common thread across all these processes—end-to-end visibility of the entire network is critical to identify performance chokepoints or areas of underutilization. Proper capacity planning requires continuous assessments of utilization, volumetric and traffic type distribution, all of which rely on comprehensive network visibility.

When it comes to enhancements and new deployments, proactive capacity planning can help IT maximize their investment dollars.

How Observer Helps with Capacity Planning

- **Assess utilization**, volumetric, and traffic type distribution with enriched flow information
- **Gain visibility** into which sites need attention or network enhancements with site-based End User Experience scoring—partitioned by location or department
- **Access Layer 2 and 3** for insights into the network including MAC addresses, IP addresses, username info, and app usage details in one, comprehensive visualization



User Experience

Drilldown	Site	User Experience Score
⬇	Eningen	0.4
⬇	Newbury	1.5
⬇	Suzhou	1.8
⬇	Eden Prairie	
⬇	*Not Defined*	
⬇	Milpitas	
⬇	Sacramento	
⬇	Germantown	
⬇	Indianapolis	
⬇	Public Viavi IP Address	
⬇	Denver	

Eden Prairie

5.5

User Experience Score

Network

Score Deductions

- Round-trip network delays
- Packet loss and retransmissions preventing connection setup
- Packet loss and retransmissions delaying connection setup
- Packet loss and retransmissions slowing data transfer
- Long data transfer times at slow speeds

Client

Top Sites by Utilization

Drilldown	Site	Bits/sec
⬇	Eden Prairie	59.28M
⬇	*Not Defined*	38.323M
⬇	Santa Rosa	3.362M
⬇	Limerick Region	3.02M
⬇	Germantown	1.377M
⬇	Denver	85.163k
⬇	Bothell	19.329k
⬇	Milpitas	15.503k
⬇	Google DNS	10.937k
⬇	Sacramento	5.071k
⬇	Singapore	2.379k

Site Interfaces

Drilldown	Site	Device			Bits/sec
⬇	Eden Prairie	MinDevErnie: GigaStor			51.344M
⬇	*Not Defined*	MinDevErnie: GigaStor			16.94M
⬇	*Not Defined*	172.21.40.250			8.264M
⬇	Eden Prairie	172.21.40.250			5.164M
⬇	*Not Defined*	172.21.40.250			4.119M
⬇	Santa Rosa	MinDevErnie: GigaStor	-	0.541	3.362M
⬇	*Not Defined*	172.21.40.250	GigabitEthernet1/0/2	29.462	2.946M
⬇	*Not Defined*	172.21.42.3	GigabitEthernetTEST-221/0/1	1.937	1.937M
⬇	*Not Defined*	172.21.42.3	GigabitEthernet1/0/2	1.869	1.869M
⬇	Germantown	MinDevErnie: GigaStor	-	0.137	1.328M
⬇	Limerick Region	172.21.40.199	4763	-	1.017M

KEY TAKEAWAYS

1. By optimizing capacity planning, IT can **maximize their ROI on new enhancements and rollouts**
2. Site-based End User Experience scoring and enriched flow data makes it **easy to determine where enhancements or redesigns are needed**
3. End to end visibility into all network infrastructure devices **helps justify IT budget** spend for all levels of management

SD-WAN OVERSIGHT & POSTURE

Many organizations today are deploying SD-WAN links instead of traditional WAN solutions. The SD-WAN vendors offer native monitoring capabilities, but they are limited in scope and capabilities. So, when there is a performance issue, and the vendor(s) assure you it is not their system, what is your recourse?

Remember, regardless of the their monitoring features, these vendors have a very narrow view with no awareness outside the SD-WAN tunnel.

SD-WAN deployments are typically approved to drive lower connectivity costs and increase business productivity. However, these objectives are not a given—it is important to validate operational and business objectives are achieved and keep the vendor(s) you selected honest in their claims of improvements.

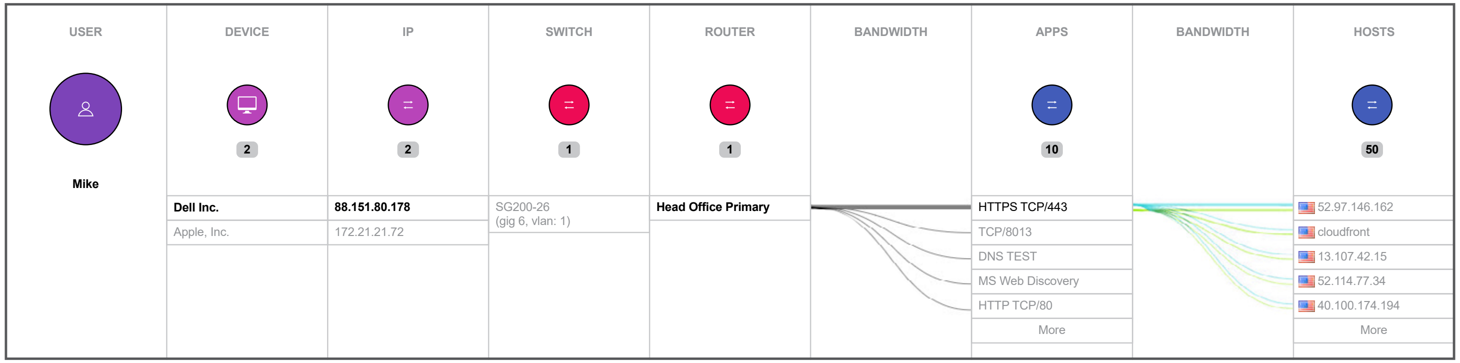
Eliminating the back and forth blame game headaches should they not requires end-to-end awareness of every user transaction.

DID YOU KNOW?

More than half of those that have or plan to have SD-WANs in place plan to use multiple vendors to do so according to the 2020 VIAVI State of the Network Survey.

SD-WAN deployment management using Observer

- **Determine whether the root cause** is associated with the SD-WAN implementation using problem domain isolation and End User Experience scoring
- **Analyze traffic volumes, composition, and prioritization** before and after SD-WAN implementation.
- **Put an end to the finger-pointing** by using forensic level network conversations as concrete evidence from the same platform



USER	DEVICE	IP	SWITCH	ROUTER	BANDWIDTH	APPS	BANDWIDTH	HOSTS
	2	2	1	1		10		50
Mike								
	Dell Inc.	88.151.80.178	SG200-26 (gig 6, vlan: 1)	Head Office Primary		HTTPS TCP/443		52.97.146.162
	Apple, Inc.	172.21.21.72				TCP/8013		cloudfront
						DNS TEST		13.107.42.15
						MS Web Discovery		52.114.77.34
						HTTP TCP/80		40.100.174.194
						More		More

KEY TAKEAWAYS

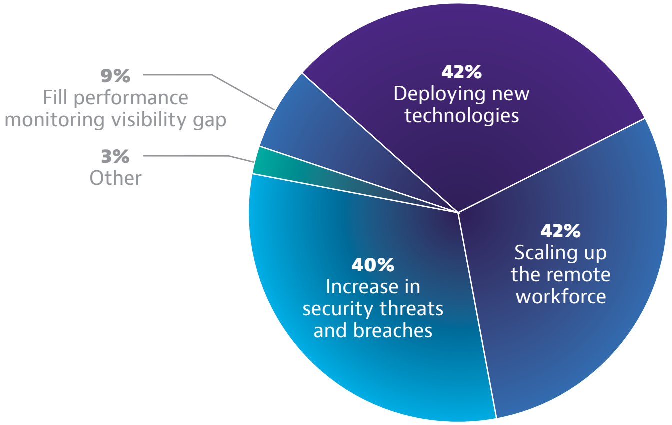
1. Observer compares performance of on-premises hosted applications before and after SD-WAN rollout to assure smooth success of SD-WAN deployment
2. By putting an end to the blame game with problem domain isolation and End User Experience data, you can maximize ROI from your SD-WAN deployment

NEW DEPLOYMENT ROLLOUTS

Imagine the application team is deploying a new service. Halfway through a lengthy deployment process, a third of the end users are left with severely impaired service. The complaints are pouring into the helpdesk. How do you exonerate the network while also aiding the IT troubleshooting process with domain specific problem root-cause isolation?

Rollouts take time and resources — whether they be cloud migrations, O365 deployments, or even hardware updates for routers, firewalls, or switches. This can quickly become a challenging support endeavor involving multiple IT personnel from Support, DevOps and NetOps if the end user's experience is affected after deployment rollout.

If you can do this in an deliberate, streamlined manner, then you can **reduce deployment costs** and **harmonize cross-team collaboration and efficiency**.

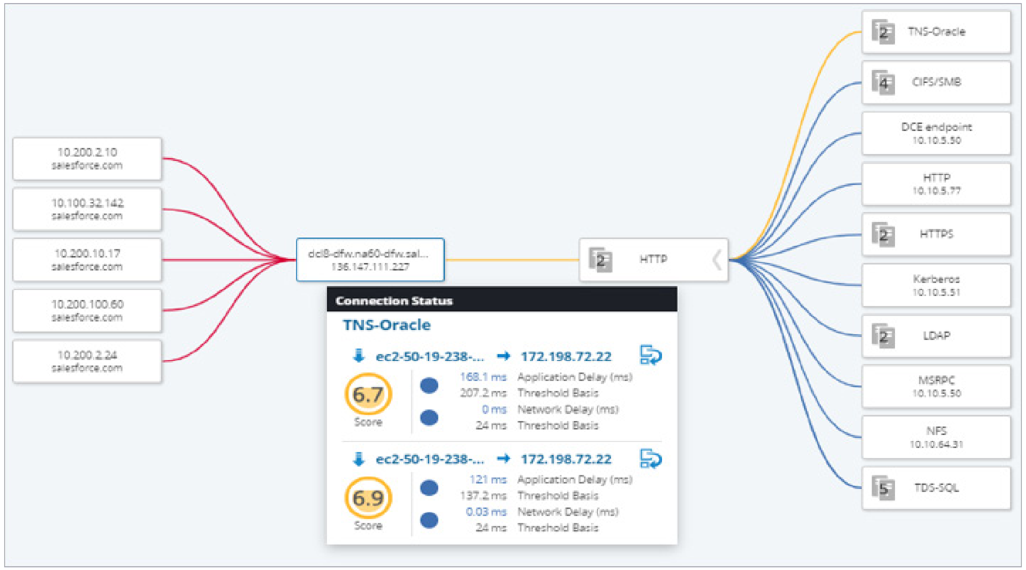


What is the biggest driver of IT budget increase?

Source: 2020 State of the Network Report from VIAVI Solutions

Ensuring Successful New Deployment Roll-out using Observer

- **Provide visibility** into the end user experience before and after deployment rollout with the patent-pending aggregated End User Experience Score
- **Identify root cause** in a multi-tier application with on-demand application dependency mapping to determine if and where the network can be rearchitected to address the performance issue
- **Validate if packets are dropped** by applications versus the network with full-fidelity network forensic data
- **Gauge "normal" performance** with baselining to identify any loss in performance after rollout



Connection Status

TNS-Oracle

ec2-50-19-238-... → 172.198.72.22

6.7 Score

168.1 ms Application Delay (ms)
207.2 ms Threshold Basis
0 ms Network Delay (ms)
24 ms Threshold Basis

ec2-50-19-238-... → 172.198.72.22

6.9 Score

121 ms Application Delay (ms)
137.2 ms Threshold Basis
0.03 ms Network Delay (ms)
24 ms Threshold Basis

KEY TAKEAWAYS

1. End User Experience scoring will help you identify issues to remedy before and after rollout.
2. Full-fidelity network forensic data can help you validate whether a performance issue is due to the network or an application.
3. Streamlining root cause of network and application issues, you can deploy new applications with minimal disruption.

To see the VIAVI Observer Platform in action, visit
viavisolutions.com/observerdemo

VIAVI Solutions

Contact Us **+1 844 GO VIAVI** (+1 844 468 4284)

To reach the VIAVI office nearest you, visit **viavisolutions.com/contacts**

viavisolutions.com/ptv