LiveAction

Unmatched Network Visibility

5 Criteria for Choosing an NPM Solution

Webinar

LiveAction Unmatched Network Visibility

ع الله (۲۵ مع ۱۹ مع الله (۲۹ مع ۱۹۹۹ مع	Application Performance Optimization
De0/2005 Sense	Accelerated Troubleshooting
FitLand/gload Display	Network Readiness Assessment
Constrainting Alline Constrainting Alline Constrainting Alline Constrainting Alline Constrainting Alline Constrainting Alline Data Data Data Data Data Data Data Data 12 0 0 Data Data Data Data 19 0 0 Data Data Data Data 19 0 0 Data Data Data	Data-Driven Change Initiatives
Image:	Advanced Reporting & Analytics
Appels D D Parallel (March 2014) D D Appels 0 0 0 0 0 0 Tests 0 0 0 0 0 0	Operational Excellence



Today's Panelists



Timothy Rhodes Managing Director Apprize360 Intelligence



David Izumo Principal Technical Marketing Engineer LiveAction

Be sure to join the conversation! Post your questions to the Q&A Panel



Criteria for Selecting an Enterprise Network Performance (NPM) Solution

Analysis of SolarWinds, Riverbed, LiveAction, and NetScout

February 2021



4

CONFIDENTIAL - DO NOT DISTRIBUTE

Study Findings

- Aggregate analysis of customer interview
- Written report available at: www.LiveAction.com



Five Criteria for Choosing an Enterprise Network Performance Management (NPM) Solution

Enterprises understand that their network is no longer a collection of technology assets but a critical component of their business strategy. In order for IT to provide strategic value to the business, you need tools that proactively ensure the reliability of network service while simultaneously boosting user experience. This requires a new approach to network management, including selecting a network-management vendor that can meet modern IT and business requirements.

To select network performance management (NPM) solutions, enterprises must push beyond the traditional selection criteria, which focus on threshold-based alerts and alarms.

If your team is considering an NPM platform—including LiveAction, SolarWinds, Riverbed, or NetScout before deciding on your vendor, consider these five criteria.

- Comprehensive end-to-end network visibility and performance management is the solution able to monitor the entire network, including SD-WAN, LAN, cloud, wireless, campus, and datacenter, or only specific categories and environments?
- Network traffic analysis Does the platform have deep packet capture and analytics to monitor real-time network traffic and application performance?
- Application visibility and performance monitoring Can the platform analyze and correlate data from network devices, applications, and cloud environments to manage the entire digital experience?
- 4. Enterprise-scale Can the solution monitor enterprise networks in organizations with more than 20,000 devices without performance issues or latency?
- <u>AlOps, analytics, and visualizations</u> Does the solution incorporate AlOps for advanced anomaly detection and correlation and visualizations that enable easy understanding of monitored environments?
- Is the solution able to monitor and manage the entire network or only specific categories or environments? Does the platform manage the entire digital experience and monitor and manage the cloud, writeless. Shu WM, LAN, application, campus, and dissonter environments?

The modern IT infrastructure is more complex than ever and encompasses a range of components that work individually and collectively to improve network performance, support productively, and encure a positive digital experience. While local technology stacks have increased in density, comparies have also expanded their infrastructure into third party SasS applications that make it a challenge to maintain comprehensive visibility. Let's suppose a unigite component is suffering from performance issues. The effects can be wide-reaching, and the cataliyst of the resulting problems can be challenging to pinpoint across such a wide range of moving parts. This is why modern IVMs follows must be able to only monitor three individual components and environments in a single solution but also correlate collected performance data to quickly identify not causes and understand their potential effects on individual environments and the overall digital experience.

An effective modern NPM solution needs to collect and correlate performance data from the entire network, often from highly complex hybrid environments. This includes monitoring all types of network devices used, wireless components, SD-WAN, LAN, cloud environments, customer and enterprise applications, VoIP devices, and the datacenter. The solution needs to collect and analyze data not only for root-cause and performance analytics but also proactive health metrics. Key health analysics include top network users, availability, common traffic patterns that contribute to performance issues, application jittler, latency, and loss. Finally, NPM solutions should automatically create baseline and trending metrics to ensure that capacity issues do not contribute to downtime or performance issues.

Does the vendor's platform support granular, correlated network-traffic insights? Does the vendor's platform have the ability to correlate traffic insights with application performance and user experience?

Whether users are accessing applications hosted internally or in the cloud, an NPM tool should correlate traffic data in real time with application performance and end-user experience. Doing this enables network operations teams to be much more efficient. Rather than analyzing every fault that the monitoring tools detect, engineers can

nd-user experience. Doing this enables network operations ng every fault that the monitoring tools detect, engineers can				
AlOps Michina learning for next-parseration baselining & predictive insights on network & application performance	٠			0
Enterprise Performance Proven security & performance with greater than 20.000 devices	•	9	•	•

Minor Functionality (- 20%)

SolarWinda

Netformance Netflow Traffic Analyzer (NTA)

NeAction

ALLWING ALLWING

O Feature Alexand (2%)

NetScout

nGeniusOne &

0

Riverbed

Riverbed Riverbed AppResponse

0

0

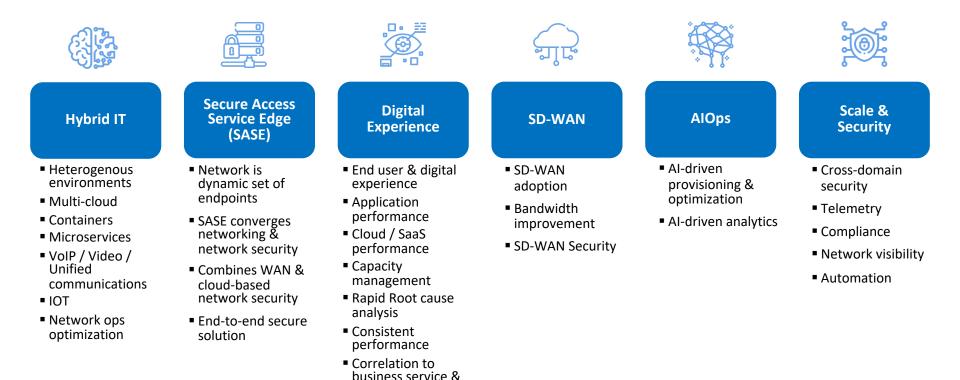
0

Buyers' NPM Evaluation Criteria

- Buyer reported criteria used to select a Network Performance Management (NPM) solution from the following vendors:
 - SolarWinds
 - ✤ LiveAction
 - ✤ NetScout
 - Riverbed

State of NPM

Six Trends shaping NPM



revenue



Does the vendor's platform provide comprehensive, end-to-end network visibility & performance management

Does the vendor's platform provide comprehensive, end-to-end network visibility & performance management



Is the solution able to support granular, correlated network traffic analysis & insights?

Does the vendor's platform provide comprehensive, end-to-end network visibility & performance management

2

Is the solution able to support granular, correlated network traffic analysis & insights?



Does the solution enable complete application visibility & performance monitoring?

Does the vendor's platform provide comprehensive, end-to-end network visibility & performance management

2

Is the solution able to support granular, correlated network traffic analysis & insights?

3

Does the solution enable complete application visibility & performance monitoring?



Is the solution capable of monitoring enterprise networks in organizations without performance issues?

Does the vendor's platform provide comprehensive, end-to-end network visibility & performance management

Is the solution able to support granular, correlated network traffic analysis & insights?

Does the solution enable complete application visibility & performance monitoring?

Is the solution capable of monitoring enterprise networks in organizations without performance issues?



Δ

Does the solution incorporate AIOps to enable advanced anomaly detection & correlation as well as visualizations to aid in the understanding of monitored environments?



Does the vendor's platform provide comprehensive, end-to-end network visibility & performance management

- Monitor & manage the entire network SD-WAN, Cloud environments, wireless devices, datacenters, VoIP, and applications
- Create automate baselines & trending metrics
- Health analytics
- Fault management
- Root cause analysis
- Performance insights

1

Does the vendor's platform provide comprehensive, end-to-end network visibility & performance management

Customer feedback

- LiveAction collects real-time data from multi-vendor network elements, including cloud, SD-WAN, applications, and datacenter
- LiveAction's LiveNA platform automatically identifies anomalies and surfaces the most critical ones to address.
- LiveAction's LiveNX supports real-time visualization of end-to-end application flows, identifying performance metrics and highlighting path changes routing changes to enable rapid diagnosis and correction.
- LiveAction supports the need for immediate troubleshooting of multi-domain performance issues as well as proactively optimizing network performance.

"APM was one of the capabilities we wanted integrated into our NPM solution, not an add-on or separate integration. Other vendors have several modules that are not integrated together. What I loved about LiveAction was that LiveWire and LiveNX had deep integration to be able to have correlated end-user experience with other environments, whether it was cloud, virtual, or network devices." –Senior network engineer, Large US Retailer

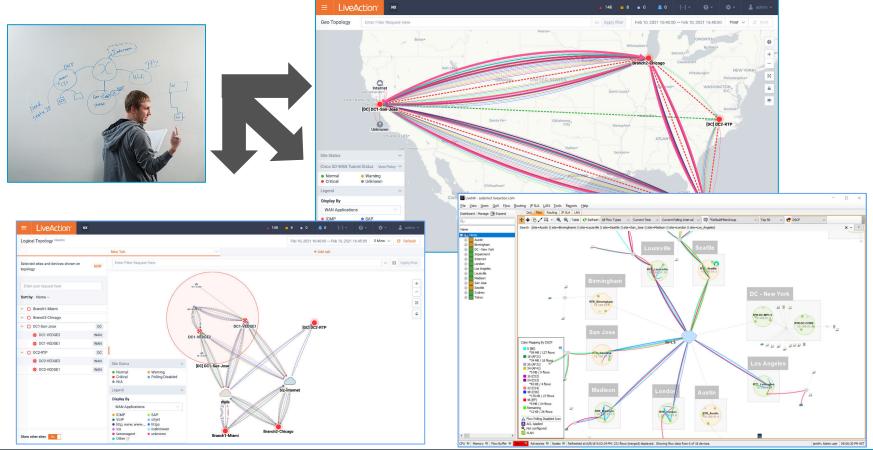
LiveNX End to End Visibility

- LiveNX Goal: Recreate the mental model of the network engineer
- Why important?
 - Networks are complex!
 - Faster troubleshooting
 - Help to operationalize new technology
 - Intuitive workflows to manage SD-WAN, cloud and the entire network





Whiteboard to Network Visibility

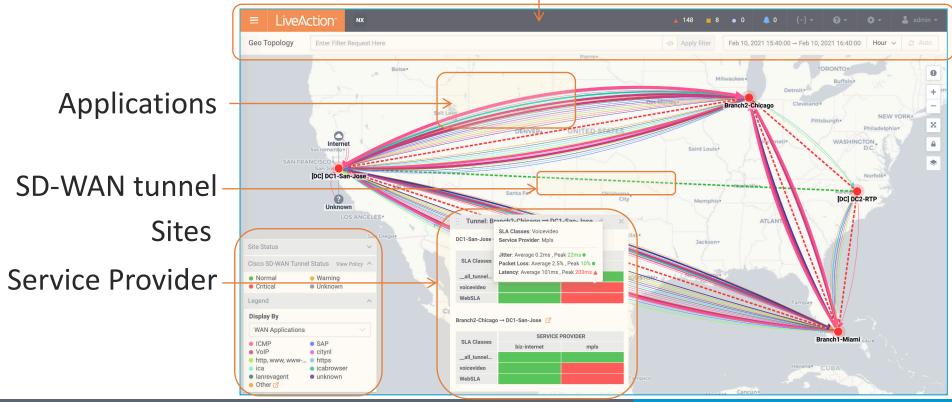


LiveAction

'18/21 Slide 1

SD-WAN Workflows: 3-Click Investigation

Operations Dashboard





Click 2: Isolate site to site data flows

Status





Click 3: Service Provider performance monitoring

	≡ LiveActio	× The					▲ 20	04 📕 18 🔹 0 🌲 262	{} 🖵 🕝	• • •	💄 admin 👻			
	< View Reports							Create Report						
	Report	Templates	DC1-San-Jose→Branc	12-Chicago Reports by Service	Provider mpls		View Opti	ons ~ Share Print	Schedule	Jse As Template	Close			
	Q Search													
	🕀 Status/Health		Application (Flow)								10			
	H Flow			ay Filter: *Hide-SD-WAN-Control Direction: 0 : Jun 08, 2018 09:20:00 HST (GMT-10:00) E				w.lp.site.src="DC1-San-Jose" & flow.lp.site.dst	="Branch2-Chicago" & wan & site="	'DC1-San-Jose" & sp="mp	ls"			
	SNMP		400							icabrowser ICMP	=			
	🕀 IPSLA		(sdq)) a 200							VoIP sip	- 1			
	🕀 Cisco SD-WAN		Bit Rate			7		Galactica SAP						
	Alerts		0 09:2009	25 09:30 09:35	09:40	09:45 09:50	09:55 10:00	10:05 10:10	10:15 10:20	quantcast dns Total				
			<pre>«< Page 1 /2 >>»</pre>						Q Search		1 £			
Service			Legend 🗘 Application	t ♦ Total Flows ♦	Total Bytes 🗘	Total Packets 🗘	Average Bit Rate 🛇	Average Packet Rate 🛇	Peak Bit Rate 🛇	Peak Packet Rate	0			
JEIVIC			icabrowse	40	37.26 MB	171,698	82.80 Kbps	47.69 pps	166.13 Kbps		95 pps			
	•		ICMP VolP	81	19.09 MB 16.55 MB	77,301	42.41 Kbps 36.77 Kbps	21.47 pps 21.48 pps	64.06 Kbps 56.32 Kbps		32 pps			
Interrupt	ion		sip	80	1.85 MB	13,600	4.12 Kbps	3.78 pps	6.22 Kbps		32 pps 5 pps			
		<u> </u>	rtp	119	1.05 MB	9,590	2.33 Kbps	2.66 pps	4.07 Kbps		4 pps			
			rdp	44	633.76 KB	2,437	1.41 Kbps	0.68 pps	3.17 Kbps		2 pps			
	(SAP	108	473.21 KB	2,890	1.05 Kbps	0.80 pps	2.18 Kbps		1 pps			
A			ica guantcast	397	290.01 KB 279.51 KB	3,274	0.64 Kbps 0.62 Kbps	0.91 pps 0.15 pps	1.18 Kbps 4.15 Kbps		1 pps 0 pps			
ADD —			dns	21	8.94 KB	21	0.02 Kbps	0.13 pps	4.13 Kbps 192 bps		0 pps			
App Details														



Click 3: Root Cause

	≡ LiveAction [™] ™							▲ 20	14 🗖 18 🖣	0 🔔 262	{}	9 - 0 -	🌣 👻 💄 admin 👻
	< View Reports	Create Report										eate Report	
	Report Templates	Tunnel SLA Class Performance Time Series (Cisco SD-WAN)									1		
	Q Search		ies Source Site: DC1-San-Jose 22:00:00 HST (GMT-10:00) End			ch2-Chicago Destina	ation Service Provider:	All Service Providers	Sia Class: All SLA	Classes Sort By: Pe	ak Round Trip Delay		
Path	🕀 Status/Health	(j 300 - wolevideu/172.16.10.2/172.16.42 = wests.4/172.16.10.2/172.16.42 =										ideo/172.16.10.2/172.16.4.2	
	Flow	di 200			\rightarrow								LAV172.16.10.2/172.16.4.2 ideo/172.16.12.2/172.16.4.2 LAV172.16.12.2/172.16.4.2 unnels_/172.16.10.2/172
Delay	SNMP	L Punog 100											unnels_/172.16.12.2/172
Delay		жее 0 22:00	22:05 22:10	22:15	22:20 22:25	22:30	22:35	22:40	22:45	22:50	22:55	23:00	
	Cisco SD-WAN Alerts						1000				Q Search		
		nd 🗘 Src Site 🗘	Src Service Provider 🗘	Dst Site 🗘	Dst Service Provider 🗘	Group 🗘	Jitter Status 🗘	Peak Jitter 🛇	Loss Status 🗘	Peak Loss Rate	Round Trip	Delay Status	Peak Round Trip Delay 🛇
• ••		DC1-San-Jo	e mpls	Branch2-Chicago	mpls	voicevideo	Normal	22 ms	Normal	10	% Critical		203 ms
Severity –		DC1-San-Jo	e mpls	Branch2-Chicago	mpls	WebSLA	Normal	22 ms	Normal	10	% Critical		203 ms
Sevency		DC1-San-Jo		Branch2-Chicago		voicevideo	Normal	24 ms			% Critical		202 ms
		DC1-San-Jo DC1-San-Jo		Branch2-Chicago Branch2-Chicago		WebSLA	Normal	24 ms			% Critical % Normal		202 ms 203 ms
		DC1-San-Jo		Branch2-Chicago Branch2-Chicago		_all_tunnels_ _all_tunnels_	Normal		Normal		% Normal		203 ms
		Site to Site Jitter/Lo	s by Service Provider (Flow)										2 G
			erface: All Interfaces Display Fil rc="DC1-San-Jose" & flow.ip.site.de							ime: Jun 07, 2018 23:00	:00 HST (GMT-10:00	Bin Interval: 5 m	inutes
		t Percentage (%) 0										—— Total	=
		22:00	22:05 22:10	22:15	22-20 22-25	22:30	22:35	22:40	22:45	22:50	22:55	23:00	
		Site to Site Applicati	n Response Time (Flow)										1 17
			erface: All Interfaces Display Fil							at Jun 07 2018 22:00-00	1 HST (GMT-10-00)	Bin Interval: 5 minu	291
			rc="DC1-San-Jose" & flow.ip.site.ds							a: Jun 07, 2018 23:00:00) HST (GMT-10:00)	Bin Interval: 5 minu	tes



2

Is the solution able to support granular, correlated network traffic analysis & insights?

- Deep packet capture & analysis
- Network traffic monitoring
- Application performance
- Transaction correlation with end-user sessions
- Pinpoint and prioritize performance issues impacting revenue

2

Is the solution able to support granular, correlated network traffic analysis & insights?

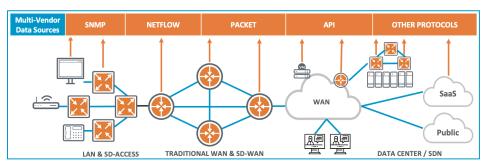
Customer Feedback

- Real-time, complete packet-by-packet analysis
- Complete network visibility ingesting packet data, flow data, WI-FI data, & device data
- LiveNX ingests flow data, including NetFlow, IPFIX, sFlow, jFlow, and data generated by LiveWire, for visibility into network performance across multi-vendor, multi-domain and multi-cloud networked environments.
- LiveWire extends functionality to include capturing packets that are traversing the wire into flow data, which is then consumed by LiveNX for in-depth performance analytics and visualization.

"LiveAction's platform takes a step by step look at your traffic, via NetFlow export. The traffic is sampled throughout its flow through your network and makes QOS, route, and security recommendations that can be implemented automatically, or one at a time with a point and click. The detail is amazing!" - Senior network engineer, Private Airline Service

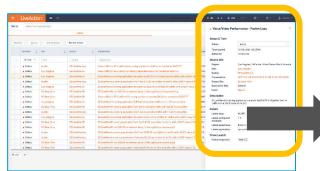
LiveNX: Multi-Telemetry For Complete Picture of Network

- LiveNX consumes vast amounts of telemetry:
 - SNMP
 - Flow: IPFIX, NetFlow, sFlow
 - Packets
 - API to SDN Controllers and Services
- Why is this important?
 - Many enterprises have point solutions that are difficult to correlate.
 - LiveNX is a single platform to manage and troubleshoot the network from the campus, WAN, cloud, data center and SD-WAN.
- Example Use Case: Voice Troubleshooting and Correction



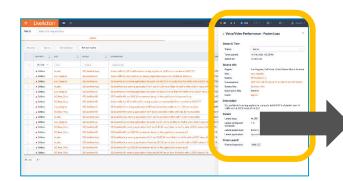


Use Case: Voice Issue - Alert > Path Analysis > Packets > Fix



Status: Active Time opened: 10 Feb 2021, 05:25PM Active for: 13 minutes Source Info Region: Los Angeles, California, United States, North America Site: Los_Angeles Device: SE-LiveWire-LA Conversation: UDP 192.168.10.202:5012 to 208.73.56.155:1200 Source Site: DC-New_York Destination Site: Internet Event: Report Description SE-LiveWire-LA running application rtp-audio had 84.33 % of packet loss for traffic with a DSCP value of 46 (EF) Datatest dscp: 46 (EF) Latest dscp: 46 (EF) Latest configured 1 % threshold: Iteration Latest packet loss: 77.77 % Latest application: rtp-audio Cross Launch Packet Inspection	Status & Time		
Active for: 13 minutes Source Info Region: Los Angeles, California, United States, North America Site: Los_Angeles Device: SE-LiveWire-LA Conversation: UDP 192.168.10.202:5012 to 208.73.56.155:12000 Source Site: DC-New_York Destination Site: Internet Event: Report Description SE-LiveWire-LA running application rtp-audio had 84.33 % of packet loss for traffic with a DSCP value of 46 (EF) Details Latest dscp: 46 (EF) Latest onfigured 1 % threshold: Tp-audio Latest application: rtp-audio Cross Launch Tp-audio	Status:	Active	
Source Info Region: Los Angeles, California, United States, North America Site: Los_Angeles Device: SE-LiveWire-LA Conversation: UDP 192.168.10.202:5012 to 208.73.56.155:12000 Source Site: DC-New_York Destination Site: Internet Event: Report Description SE-LiveWire-LA running application rtp-audio had 84.33 % of packet loss for traffic with a DSCP value of 46 (EF) Details Latest dscp: Latest dscp: 46 (EF) Latest configured 1 % threshold: T7.77 % Latest application: rtp-audio Drilldown to packets	Time opened:	10 Feb 2021, 05:25PM	
Region: Los Angeles, California, United States, North America Site: Los_Angeles Device: SE-LiveWire-LA Conversation: UDP 192.168.10.202:5012 to 208.73.56.155:12000 Source Site: DC-New_York Destination Site: Internet Event: Report Description SE-LiveWire-LA running application rtp-audio had 84.33 % of packet loss for traffic with a DSCP value of 46 (EF) Details Latest dscp: 46 (EF) Latest dscp: 46 (EF) Latest packet loss: 77.77 % Latest application: rtp-audio Cross Launch	Active for:	13 minutes	
Site: Los_Angeles Device: SE-LiveWire-LA Conversation: UDP 192.168.10.202:5012 to 208.73.56.155:12000 Source Site: DC-New_York Destination Site: Internet Event: Report Description SE-LiveWire-LA running application rtp-audio had 84.33 % of packet loss for traffic with a DSCP value of 46 (EF) Details Latest dscp: 46 (EF) Latest qacket loss: 77.77 % Latest application: rtp-audio Cross Launch Internet	Source Info		
Device: SE-LiveWire-LA Conversation: UDP 192.168.10.202:5012 to 208.73.56.155:12000 Source Site: DC-New_York Destination Site: Internet Event: Report Description SE-LiveWire-LA running application rtp-audio had 84.33 % of packet loss for traffic with a DSCP value of 46 (EF) Details Latest dscp: 46 (EF) Latest configured 1 % threshold: Latest application: rtp-audio Cross Launch	Region:	Los Angeles, California, United States, North Americ	ica
Conversation: UDP 192.168.10.202:5012 to 208.73.56.155:12000 Source Site: DC-New_York Destination Site: Internet Event: Report Description SE-LiveWire-LA running application rtp-audio had 84.33 % of packet loss for traffic with a DSCP value of 46 (EF) Details Latest dscp: 46 (EF) Latest configured 1 % threshold: Latest packet loss: 77.77 % Latest application: rtp-audio Cross Launch	Site:	Los_Angeles	Drilldours fo
Source Site: DC-New_York Destination Site: Internet Event: Report Description SE-LiveWire-LA running application rtp-audio had 84.33 % of packet loss for traffic with a DSCP value of 46 (EF) Details Latest dscp: 46 (EF) Latest configured 1 % threshold: Latest packet loss: 77.77 % Latest application: rtp-audio	Device:	SE-LiveWire-LA	Drilldown fo
Source site. DC-New_TOIX Destination Site: Internet Event: Report Description SE-LiveWire-LA running application rtp-audio had 84.33 % of packet loss for traffic with a DSCP value of 46 (EF) Details Latest dscp: 46 (EF) Latest configured 1 % threshold: Latest packet loss: 77.77 % Latest application: rtp-audio Cross Launch DC-New_TOIX DC-NEW	Conversation:	UDP 192.168.10.202:5012 to 208.73.56.155:12000	more detail
Event: Report Description SE-LiveWire-LA running application rtp-audio had 84.33 % of packet loss for traffic with a DSCP value of 46 (EF) Details Latest dscp: 46 (EF) Latest configured 1 % threshold: Latest packet loss: 77.77 % Latest application: rtp-audio Cross Launch Image: Construct of the second s	Source Site:	DC-New_York	more detail
Description SE-LiveWire-LA running application rtp-audio had 84.33 % of packet loss for traffic with a DSCP value of 46 (EF) Details Latest dscp: 46 (EF) Latest configured 1 % threshold: Latest packet loss: 77.77 % Latest application: rtp-audio Cross Launch	Destination Site:	Internet	
SE-LiveWire-LA running application rtp-audio had 84.33 % of packet loss for traffic with a DSCP value of 46 (EF) Details Latest dscp: 46 (EF) Latest configured 1 % threshold: Latest packet loss: 77.77 % Latest application: rtp-audio Cross Launch Drilldown to packets	Event:	Report	
traffic with a DSCP value of 46 (EF) Details Latest dscp: 46 (EF) Latest configured 1 % threshold: Latest packet loss: 77.77 % Latest application: rtp-audio Cross Launch Drilldown to packets	Description		
Latest dscp: 46 (EF) Latest configured 1 % threshold: Latest packet loss: 77.77 % Latest application: rtp-audio Cross Launch			
Latest configured 1% threshold: Latest packet loss: 77.77% Latest application: rtp-audio Cross Launch	Details		
threshold: Latest packet loss: 77.77 % Latest application: rtp-audio Cross Launch	Latest dscp:	46 (EF)	
Latest application: rtp-audio Cross Launch		1 %	Drilldown to
Cross Launch	Latest packet loss:	77.77 %	packets
		rta audio	packets
Packet Inspection Peek 🗹	-	Ttp-audio	
	Latest application:	Црацию	

Use Case: Voice Issue - Alert > Path Analysis > Packets



Voice/Video Perf	formance - Packet Loss ×
Status & Time	
Status:	Active
Time opened:	10 Feb 2021, 05:25PM
Active for:	13 minutes
Source Info	
Region:	Los Angeles, California, United States, North America
Site:	Los_Angeles
Conversation:	UDP 192.168.10.202:5012 to 208.73.56.155:12000
Source Site.	DC-New_YOIK
Destination Site:	Internet
Event:	Report
Description	

SE-LiveWire-LA running application rtp-audio had 84.33 % of packet loss for traffic with a DSCP value of 46 (EF)

Details

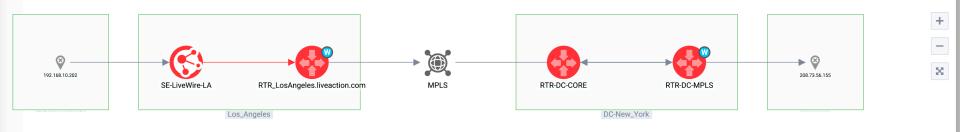
Latest dscp:	46 (EF)	
Latest configured threshold:	1 %	
Latest packet loss:	77.77 %	
Latest application:	rtp-audio	
Cross Launch		
Packet Inspection	Peek	

Drilldown to Path Analysis for the specific conversation



WAN Applications > Application: > PATH UDP 192.168.10.202 : 5012 - 208.73.56.155 : 12000

Feb 10, 2021 17:10:41 → Feb 10, 2021 17:25:41



Path Flow DC-New_York - Internet

Device Name	SE-LiveWire-LA Peek 🗹	RTR_LosAngeles.liveaction.com	RTR-DC-CO	RE RTR-DC-MPLS
Site Name	LOS	Los_Angeles	DC-New_Y	rk DC-New_York
Application		rtp-audio	r	sp statistical-conf-audio
CPU Usage	8.0.	7.00 %	7.00	% 10.00 %
Memory Usage	50.00 %		15.00	% 16.00 %
In Interface	eth1	Peek 🔽	GigabitEthern	t3 GigabitEthernet3
Out Interface	eth1	I CCK	GigabitEthern	t2 GigabitEthernet2
In QoS Policy	No Policy		No Pol	cy No Policy
Out QoS Policy	No Policy	SHAPING	No Pol	cy No Policy
Bytes In	1.56 MB	1.43 MB	693.77	KB 693.77 KB
Bytes Out	1.56 MB	693.77 KB	693.77	KB 693.77 KB
Bit Rate In	13.89 Kbp		6.17 Kt	os 6.17 Kbps
Bit Rate Out	13.89 Kbr	Drilldown to P	ackels 6.17 Kt	6.17 Kbps
Utilization In	0.00	0.00 /0	0.00	% 0.01 %
Utilization Out	0.00 %	0.01 %	0.00	% 0.00 %
Jitter Average	67.95 ms	-		
Packet Loss Rate	77.77 %	-		

Peek – Packet Analytics

LiveAction ⁻ Peek.					Live	Action [®] Peek.					
SE-LiveWire-LA / Forensic Searche	s / Bad Call - High Loss - Ron / Voi	ice & Video Dashboard			SE-Live	eWire-LA / Forensic Se	earches / Bad Call - High Loss - Ron	/ Packets			
Home Captures Forensics File	es Forensic Searches Events Ada				r# Hom	ne <u>Captures</u> Forensic	s Files Forensic Searches Events	Adapters Setting	s Admin		
Home Dashboard Captu Network Packets Applications Events Voice & Video		leo Visuals Statistics Tools Peer Map Summary Applications Compass Graphs Nodes Countries Protocols			쑭 Hor	Metwork P Applications E Voice & Video	Packets Flows Calls	Video Visuals Peer Map Graphs	Statistics To Summary Applications Co Nodes Countries Protocols	iols mpass	
Call Summary			Call Quality Distribution		Pack	cets (14,943)					
	OUNTERS	CLOSED CALL STATISTICS	All Calls	100.0% 100 ס	Ψ×	Enter a filter expressi	ion				
CURREN	T CALLS 1	VOICE PACKET LOSS 10.926%	75-	75-		PACKET SOURCE	DESTINATION	FLOW ID SIZ	E RELATIVE TIME PROTOCO	L APPLICATION	SUMMARY
	N CALLS 0 D CALLS 1	VIDEO PACKET LOSS 0.000% AUDIO PACKET LOSS 0.000%	50-	50-		1 192.168.10.18	192.168.107.11	1 21	8 0:00:00.017201 G.711	UDP	SSRC=0x97598194, Seq=11548, Time=3677666995, 20 data
AVG. CALL DU	JRATION 0:09:30	MOS-CQ 1.75	25-	25-		2 192.168.10.18	192.168.107.11	1 21	3 0:00:00.050243 G.711	UDP	SSRC=0x97598194, Seq=11549, Time=3677667155, 20 data
		MOS-A 0.00 MOS-V 0.00	0 0.0% 0.0% Good Fair	0.0% 0 Got		3 192.168.10.18	192.168.107.11	1 21	8 0:00:00.080873 G.711	RTP	SSRC=0x97598194, Seq=11550, Time=3677667315, 20 data b
		M05-V 0.00	Good Fair	Poor Bad Got		4 192.168.10.18	192.168.107.11	1 21	3 0:00:00.143170 G.711	RTP	SSRC=0x97598194, Seq=11552, Time=3677667635, 20 data
Call Quality 10 Second Average						5 192.168.10.18	192.168.107.11	1 21	8 0:00:00.174927 G.711	RTP	SSRC=0x97598194, Seq=11553, Time=3677667795, 20 data
1-						6 192.168.10.18	192.168.107.11	1 21	0:00:00.205589 G.711	RTP	SSRC=0x97598194, Seq=11554, Time=3677667955, 20 data
					•	7 192.168.10.18	192.168.107.11	1 21	8 0:00:00.236380 G.711	RTP	SSRC=0x97598194, Seq=11555, Time=3677668115, 20 data b
0.75-						8 192.168.10.18	192.168.107.11	1 21	8 0:00:00.268413 G.711	RTP	SSRC=0x97598194, Seq=11556, Time=3677668275, 20 data
ø 0.5-						9 192.168.10.18	192.168.107.11	1 21	0:00:00.299350 G.711	RTP	SSRC=0x97598194, Seq=11557, Time=3677668435, 20 data
Calls						10 192.168.10.18	192.168.107.11	1 21	3 0:00:00.329342 G.711	RTP	SSRC=0x97598194, Seq=11558, Time=3677668595, 20 data
0.25-											
07:28:00 07:27:10 07	:28:20 07:29:30 07:30:40 07:31:50 07	7:33:00 07:34:10 07:35:20 07:36:30 07:37:40 07:38:50 07:4 Good	0:00 07:41:10 07:42:20 07:43:30 07:44:40 0 Fair Poor Bad Unknown	17:45:50 07:47:00 07:48:10 07:49:20 07:50:30 0	Pa	et Info ocket Number:	7			0000 00 00 00 00 00 00 0010 00 C8 A7 75 0	0 0A 00 50 56 B9 68 F6 08 00 45 B8PV.hE. 0 00 3D 11 DE 89 C0 A8 0A 12 C0 A8u.= 9 DC 00 B4 CF FC 80 00 2D 23 DB 34 k.K.y#.4
Call Quality by Codec 10 Second	Average					ags: atus:	0×00800800 0×00800800			0030 C3 13 97 59 8	1 94 7D 7B 7E 78 FF FC 78 F6 7E 79Y}{~xx.~y
57					Pa	icket Length:	218	20			C F4 FF FC 76 F8 77 7F 7C FC 7F 7D x.v. v.w. } C F6 F7 7C 76 7B 75 FC 7D FD FE F8 w v{u.}
4-						mestamp: ernet Type 2	10:25:00.236379885 03/25/20	20		0060 78 FD FE 7C F	D 78 7F 7A 7C 79 F9 7A FC 7E F7 FC { .x.z y.z.~
		vice //idee D	ataila —		Des	stination:	08:08:00:00:00:00	D		0070 FD 7D F4 FC F	9 77 FE 7C 7D FE 7A 77 F4 79 7D 7B .}w. }.zw.y}{
g 3-	VC	oice/Video D	etalls			ource: otocol Type:	00:00:00:00:00:0A 00:50:55:B9:68:F6 0x0800 Internet Pro	W P	ackets a	76 N F C	B C 7E 7F 7D FB 78 7C F7 7B FF v . ~.}.x .{.
X							Internet Protocol Datagram	51.m (1P(1))		00A0 /A /A /B F4 /	6 F6 FD FB 75 F9 7D F3 78 FD 7D FC zz{.vu.}.x.}.
2-					Vei	rsion:	4 [14 Mask 0xF0]				A F3 FB 7D 7A 7A 7D FC 78 F8 7D 7E v.{.z.}zz}.x.}~ E FE F4 FC 7A 7D FC 7B FC 7A FE 7A z.y.~z}.{.z.z
					nttps://1	10.100.51.38/omnipeek/c	aptures to America and				



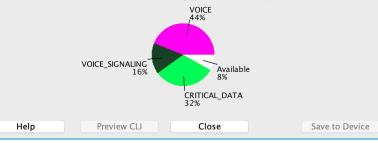
Fix: QoS Monitoring and Configuration

Add Bandwidth to VOICE Class



Adjust Nested Output Policy 'SHAPING / QUEUEING' on RTR_LosAngeles.liveaction.com (1... Bandwidth Allocation by Class Class Name **Oueue Settina Reserved Bandwidth** Other Settings \$ **Priority Oueueing** Kbps VOICE 88 Class-based Queueing 32 VOICE SIGNALING Kbps Class-based Queueing $\hat{}$ 64 Kbps CRITICAL DATA class-default None Bandwidth Summary by Interface Shape link to: 200 Kbps Average Percent using Interface Bandwidth (Kbps) Shaped (Kbps) **Reserved** (Percent) GigabitEthernet2 / Output 92.00% 1.000.000 200

Guaranteed Bandwidth Allocation for Interface GigabitEthernet2 / Output



LiveAction

3

Does the solution enable complete application visibility & performance monitoring?

- Analyze & correlate data from network devices, applications, & cloud environments
- Visualize packet-by-packet to perform detailed application-performance analysis.
- Pinpoint the source of latency as network versus application.
- Report top application performance highlighting average application and network delays.
- Digital and end-user experience monitoring
- Synthetic user experience

3

Does the solution enable complete application visibility & performance monitoring?

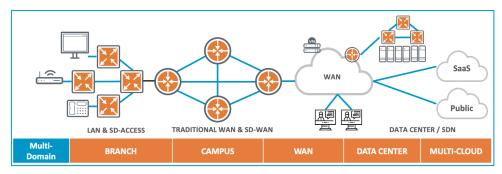
Customer feedback

- LiveAction analyzes application traffic with full visibility into protocol and application types, including video, voice, instant messaging, and file transfer.
- LiveAction enables troubleshooting of applications deployed in the datacenter, public cloud, or hybrid network.
- Provides insights into how a network is being used, how applications are performing, and which sanctioned or unsanctioned applications are being used.
- Using LiveAction's Application Path Analytics (APA) feature, users can identify precisely where application performance issues originate and correlate the impact of those issues on other applications and network devices

"One of the things that other customers told me about LiveAction was the level of detailed insights for dashboards and reporting, especially about segmenting by network traffic by type. LiveAction has very detailed filtering capabilities, which allows for this granular capture and review of different data types for RCA." – Senior Manager of Network Architecture, International CPG Manufacturer

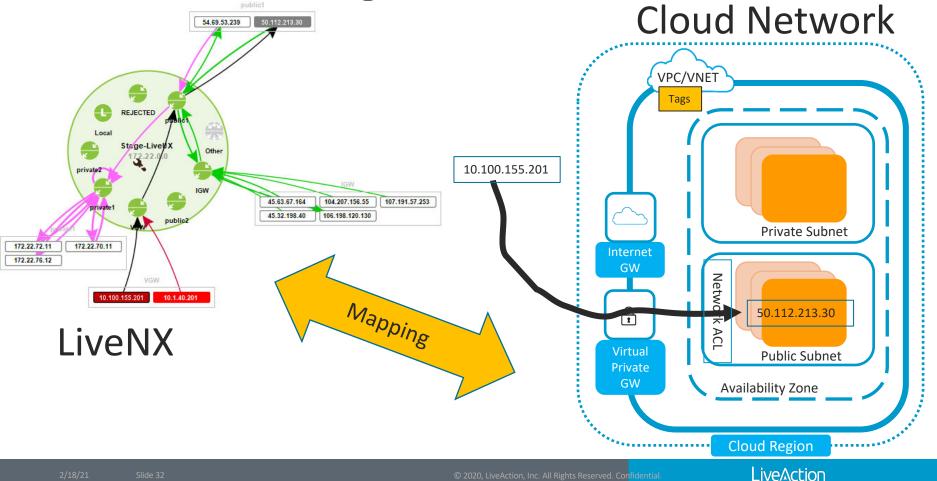
Multi-Domain Application Visibility

- Why is this important?
 - Applications are prolific
 - Apps are hosted on-premises in data centers and in the private or public clouds
 - End users and business entities don't care where the app is located. They need to drive business objectives.
- How?
 - Visibility across multi-domain and multivendor networks
- Example Use Case: Cloud Monitoring

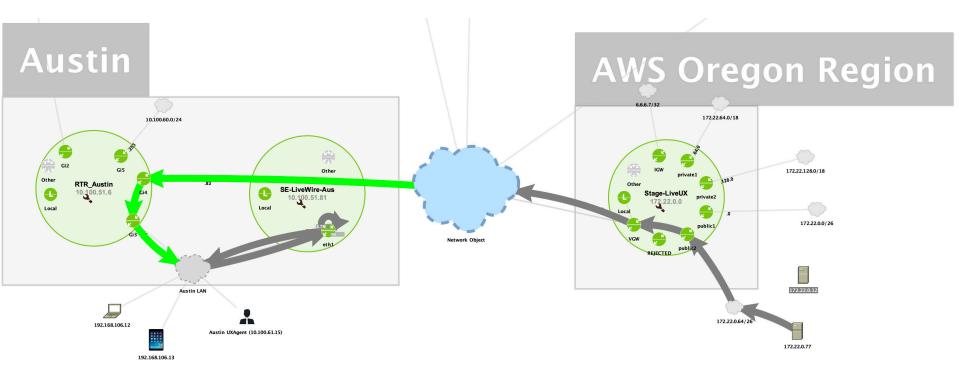




Cloud Network Through LiveNX Lens

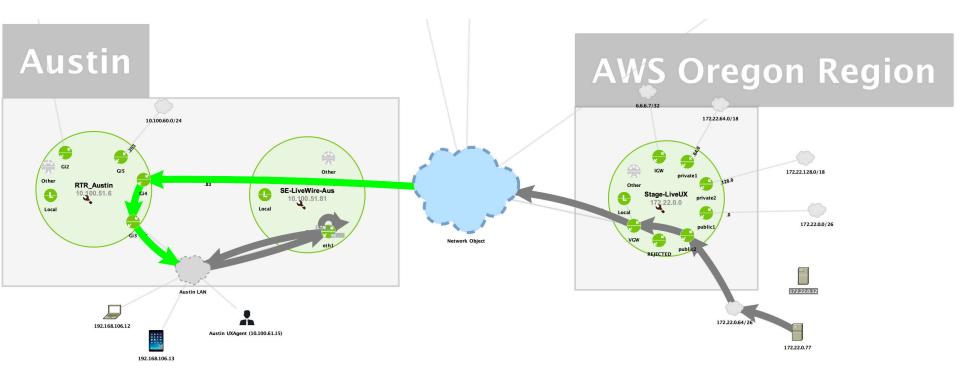


End-to-End Path Visibility via LiveNX



LiveAction

End-to-End Path Visibility via LiveNX



LiveAction



Is the solution capable of monitoring enterprise networks in organizations without performance issues?

- Monitor large-scale, complex & hybrid environments with minimal latency, including SD-WAN, multi-cloud deployments, and various application infrastructures
- Analyze capacity to help plan & predict for needed resources to maintain performance levels

4

Is the solution capable of monitoring enterprise networks in organizations without performance issues?

Customer feedback

- LiveAction can support large enterprise deployments without performance or latency issues, supporting multi-site and multi-region deployments.
- LiveAction supports real-time, detailed monitoring and network-performance management.
- In addition to supporting scale, LiveAction supports a company's growth by analyzing and supporting capacity planning to ensure that the proper number and type of resources are included to enable the required performance.

"As a large multi-national organization, we require scalable solutions that do not require patchwork to make them work across different regions or for type sizes of devices and environments. We felt like with other vendor solution we would have to deploy multiple different instances and then tie them together on the back-end to make it work across the over 100,000 devices we have in our network." – Senior Manager of Network Architecture, International CPG manufacturer

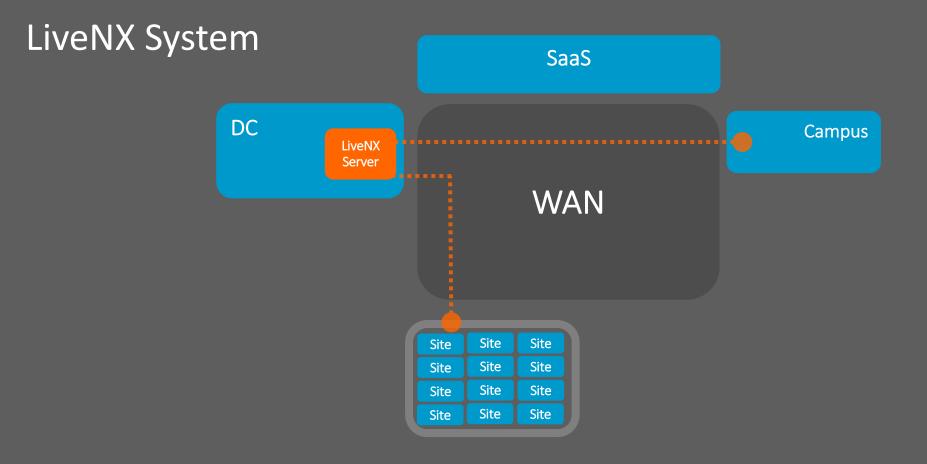
LiveNX Scale for Large Enterprise

- 100's, 1000's or 10,000s of devices
- Many sites across multiple regions
- Distributed architecture
- Horizontal scale
- Strategic packet capture

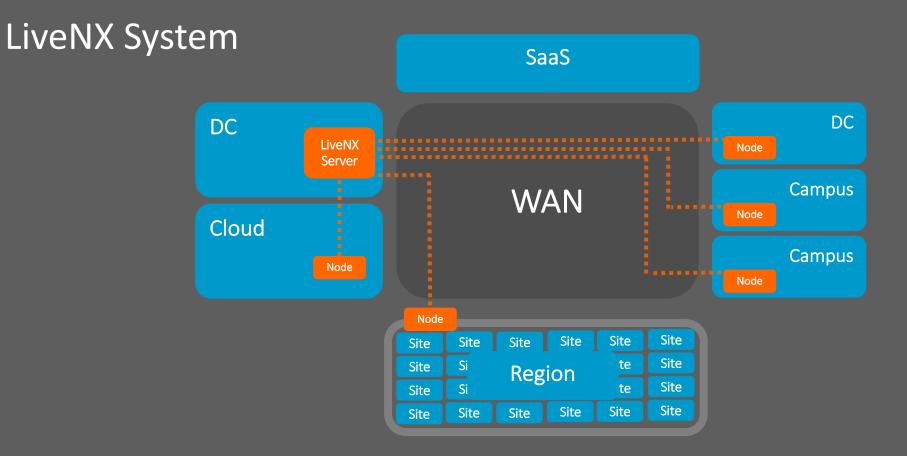
LiveNX Platform



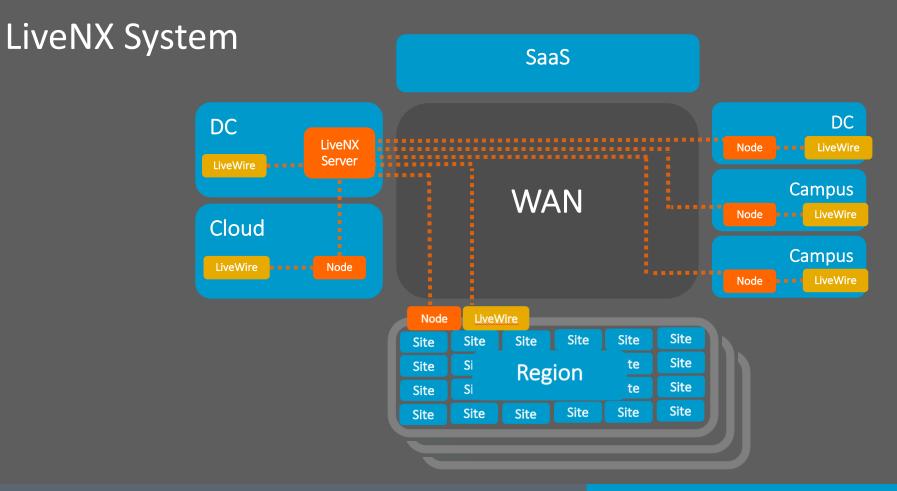




LiveAction (c) 2020



LiveAction (c) 2020



LiveAction

LiveAction (c) 2020

NPM Selection Factors

5

Does the solution incorporate AIOps to enable advanced anomaly detection & correlation as well as visualizations to aid in the understanding of monitored environments?

- Machine learning to support scalable anomaly detection, dependency mapping, & event correlation
- Algorithms that support dynamic performance correlations, including determining which voice traffic to prioritize, when to throttle bandwidth, and whether a user's access should be blocked
- Visualizations to show network performance

NPM Selection Factors

5

Does the solution incorporate AIOps to enable advanced anomaly detection & correlation as well as visualizations to aid in the understanding of monitored environments?

Customer feedback

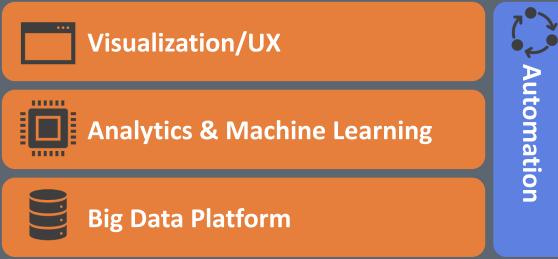
- LiveNA is LiveAction's AIOps platform, which applies machine learning and heuristics to network datasets to enable advanced anomaly detection and predictive analytics
- LiveNA uses proprietary machine-learning algorithms to establish baselines for applications and the network to detect deviations from the baseline, anomalies and correlate events.
- LiveAction's patented visualization engine provides visual insights into the entire network, including visual packet analysis, visual path analytics, transport view, virtual overlay view, and site-specific details.

"AI is kind of of getting a bad wrap right now. But what LiveAction has done has built a very intentional machine learning-based foundation for LiveNX to continuously identify patterns and insight from customer metadata and identify anomalous behavior.... We need machine learning that can analyze and discover anomalous and performance data at scale." – Senior Manager of Network Architecture, International CPG manufacturer

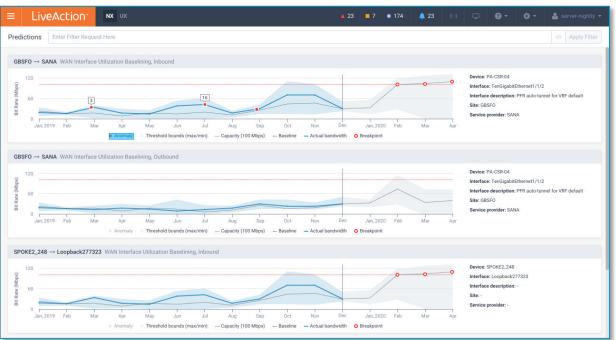
LiveNA Network AlOps Platform

Analytics & Machine Learning

- Anomaly Detection
- Predictive Analytics
- Network Understanding
- Analytics Automation
 - Decision Automation
 - Continuous Expert Analysis
- Big Data Platform
 - Multi Telemetry
 - High Scale Ingest



LiveNA Capabilities



- 1. Application Utilization and Performance Baselining – LiveNA learns the utilization and performance patterns of the top network applications, baselines them on a per device per direction bases, and detects anomalies when the utilization deviates from learned normal behavior.
- WAN Utilization Baselining and Prediction LiveNA learns WAN interface utilization, baselines it, and detects anomalies when the performance deviates from learned normal behavior. In addition, it will trend utilization and provided predictions for threshold crossing events.
- **3. QoS Utilization Baselining** LiveNA learns QoS class utilization, baselines it and detects anomalies when the performance deviates from learned normal behavior.
- Anomaly Prioritization (Summary Overview Page) Top Anomalies and Insights can be quickly understood in context per app, per site, and per device. This allows context relevant drill-down to anomaly details.
- 5. Enterprise Scale Ingestion and processing of massive enterprise data sets combined with Al driven analysis to provide anomaly detection at scale. This allows teams to be presented prioritized issues without searching through vast data sets.

Energy Company and Medical Supply Organization Drastically Saves Valuable Time

Previously, Capacity Planning would take many hours or even multiple days to gather data, create reports and hand off to management. With LiveNA's predictive analytics, network admins can log in at their convenience and with a few button clicks, clearly identify WAN circuits that need upgrades.

They can **predict** when these critical WAN links will potentially run out of bandwidth.

This new workflow resulted in significant reduction in time and effort and allows the network team to focus on driving business upgrades.







Buyers' Vendor Perceptions

- Buyer reported perceptions of vendors:
 - SolarWinds
 - ✤ LiveAction
 - NetScout
 - Riverbed

Legend				
Fully Functionality (~75%)	Partial Attionality (~50%) Functionality (~50%)	nor Fe onality (~25%) Absent (ature (0%)	
	LiveAction	SolarWinds	NetScout	Riverbed
Categories of Assessment	LiveNX, LiveWire, & LiveNA	Network Performance Monitor (NPM). NetFlow Traffic Analyzer (NTA)	nGeniusOne & Infinistream NG	Riverbed NPM and Riverbed AppResponse
End-to-End Network Performance Management Able to monitor the entire network without use of numerous modules, add-ons, and integrated partner solutions for: • Network traffic & pack analytics • SD-WAN, LUN, & Datacenter monitoring • Cloud and Application performance, wrieless & UC monitoring • End-User Experience (EUE) monitoring	•		•	•
Digital Experience Monitoring • Real-Time Insight into application & user-level activity • Synthetic user experience analysis	G		e	G
SD-WAN Monitoring • Visibility into underlays & overlays, tunnel performance, & lifecycle monitoring • Real-time visualization of end-to-end application performance	•			
Cloud monitoring • Visibility into multi-cloud environments • Ability to analyze bandwidth utilization of applications & services	e			
Application Performance Monitoring Traceability & analytics on network performance metrics from devices with application performance insights - Application path analytics - Packet-by-packet ladder analysis for detailed APM	e	G	b	•
Unified Communications Analysis & Troubleshooting Monitoring & root cause analysis of VoIP, video, & UC	•			
Cisco QoS Ability to monitor Cisco QoS class per service with real-time visualization into QoS anomalies	•		•	•
Advanced anomaly detection & correlation Leverage machine learning algorithms to create dynamic baselines & identify anomalous behavior from multiple sources of raw data	•	4		G
Alerting & Notifications Support for multi-threshold alerting rules customized by site, device, & region	L	G		
Capacity Planning Analyze & plan for additional bandwidth & processing power needs		4		
Advanced Analytics and Reporting • Easy-to-build dashboards & reports • Visualizations of network, transport, virtual overlay, packet analytics, & site-specific details	•		e	
AlOps Machine learning for next-generation baselining & predictive insights on network & application performance 	•	•	•	•
Enterprise Performance Proven security & performance with greater than 20,000 devices	•	4		G

Vendor Perceptions

Legend

Functionality (~50%)

Partial

Minor Functionality (~25%)

Feature Absent (0%)

Categories of Assessment	LiveAction	SolarWinds	NetScout	Riverbed
	LiveNX, LiveWire, & LiveNA	Network Performance Monitor (NPM), NetFlow Traffic Analyzer (NTA)	nGeniusOne & Infinistream NG	Riverbed NPM and Riverbed AppResponse
 End-to-End Network Performance Management Able to monitor the entire network without use of numerous modules, add-ons, and integrated partner solutions for: Network traffic & pack analytics SD-WAN, LAN, & Datacenter monitoring Cloud and Application performance, wireless & UC monitoring End-User Experience (EUE) monitoring 	•			
Digital Experience Monitoring Real-Time insight into application & user-level activity Synthetic user experience analysis 				e
 SD-WAN Monitoring Visibility into underlays & overlays, tunnel performance, & lifecycle monitoring Real-time visualization of end-to-end application performance 	•			
 Cloud monitoring Visibility into multi-cloud environments Ability to analyze bandwidth utilization of applications & services 	G		G	

Fully

Present

0

Partial

Functionality (~75%)

Vendor Perceptions

Legend

Partial Functionality (~50%) Minor Functionality (~25%)

%) Feature Absent (0%)

Categories of Assessment	LiveAction	SolarWinds	NetScout	Riverbed
	LiveNX, LiveWire, & LiveNA	Network Performance Monitor (NPM), NetFlow Traffic Analyzer (NTA)	nGeniusOne & Infinistream NG	Riverbed NPM and Riverbed AppResponse
 Application Performance Monitoring Traceability & analytics on network performance metrics from devices with application performance insights Application path analytics Packet-by-packet ladder analysis for detailed APM 	L	L	L	
Unified Communications Analysis & Troubleshooting Monitoring & root cause analysis of VoIP, video, & UC			L	
Cisco QoS Ability to monitor Cisco QoS class per service with real-time visualization into QoS anomalies		•	•	
Advanced anomaly detection & correlation Leverage machine learning algorithms to create dynamic baselines & identify anomalous behavior from multiple sources of raw data	•			

Fully

Present

0

Partial

Functionality (~75%)

Vendor Perceptions

Legend

Partial Minor Functionality (~50%) Functionality (~25%)

(~25%) Feature Absent (0%)

	LiveAction	SolarWinds	NetScout	Riverbed
Categories of Assessment	LiveNX, LiveWire, & LiveNA	Network Performance Monitor (NPM), NetFlow Traffic Analyzer (NTA)	nGeniusOne & Infinistream NG	Riverbed NPM and Riverbed AppResponse
Alerting & Notifications Support for multi-threshold alerting rules customized by site, device, & region	L		L	
Capacity Planning Analyze & plan for additional bandwidth & processing power needs				
 Advanced Analytics and Reporting Easy-to-build dashboards & reports Visualizations of network, transport, virtual overlay, packet analytics, & site-specific details 	•		L	
 AIOps Machine learning for next-generation baselining & predictive insights on network & application performance 				
Enterprise Performance Proven security & performance with greater than 20,000 devices			L	G

Fully

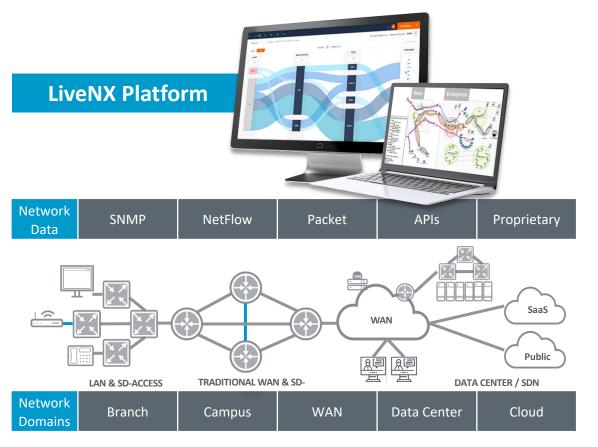
Present

0

Partial

Functionality (~75%)

How LiveAction is Different



How Can We Help?

Get the full picture and insights to choose the right NPM solution



www.liveaction.com/contact-sales/

www.liveaction.com/company/request-demo/

www.liveaction.com/download/



LiveAction

Unmatched Network Visibility

Don't miss our next Webinar: Charting a Path to Successful SD-WAN Operations

Thank you

www.liveaction.com