Telemetry Gaps: Six Approaches to Erase Your Network Blind Spots

WHITE PAPER

LiveAction®

Table of Contents

Executive Summary:

Limited network visibility can plague a business in several ways. Let's consider the most common blind spots organizations struggle with and the best approaches to close those telemetry gaps.

Common Blind Spots Challenges in a Network:

Traditional trouble spots include

- → Encryption Blind Spots
- → SD-WAN
- → Network Edges
- → Data Centers
- → Remote Sites
- → Cloud

Why Removing Blind Spots Matters for Business Objectives

Proactive Security

- → Improves security visibility and allows you to detect unauthorized access and attempt before a successful breach occurs

Resource Planning

- → Identify trends early to plan appropriately for future network needs when network devices are sputtering to a halt etc.

Capacity Planning

- → Know how and where your data is increasing any bandwidth abuse
- → Visibility lets you track bandwidth use – to see how and where it is being used – this lets you make plans about increasing bandwidth

Less Downtime

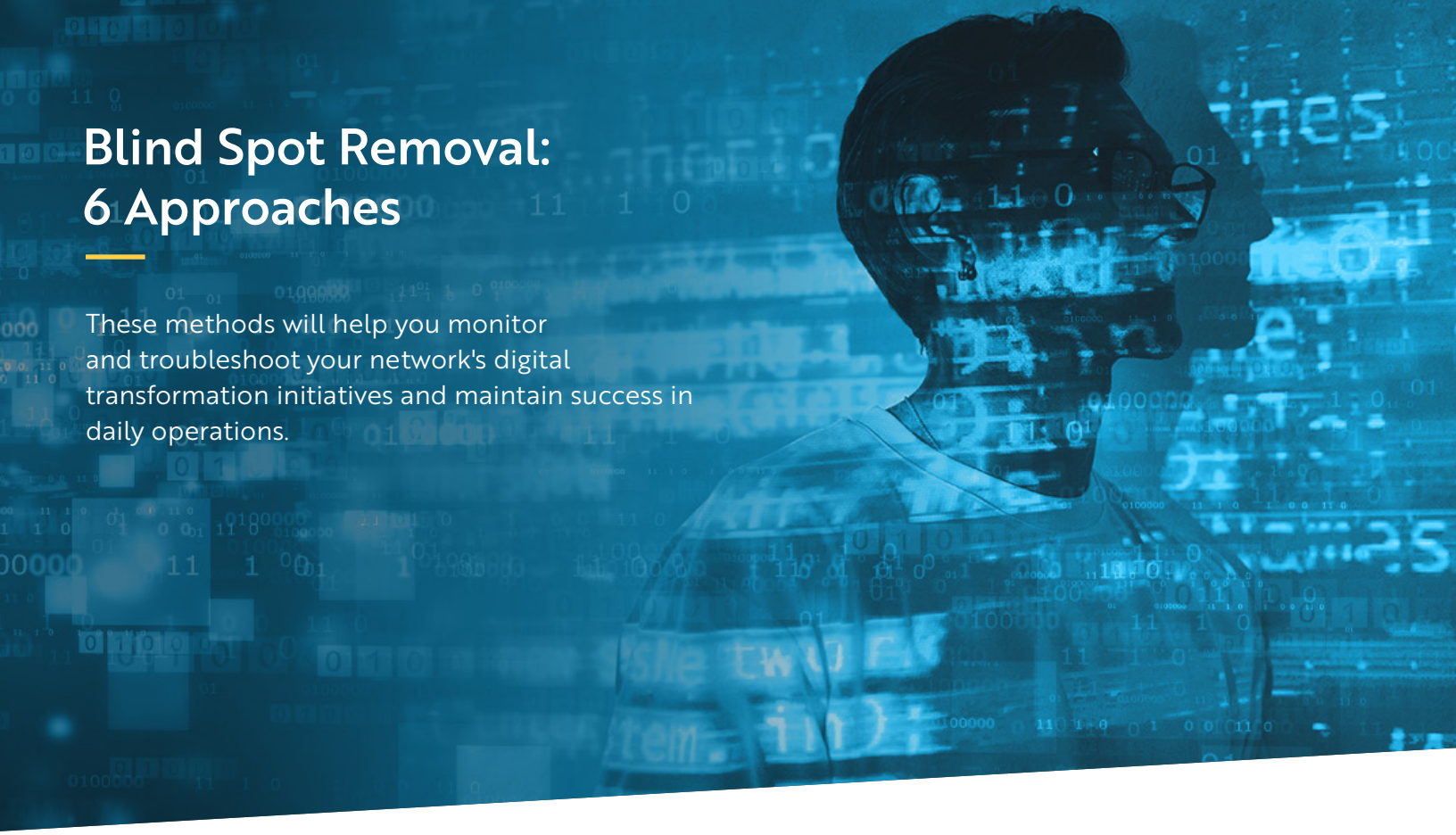
- → Visibility lets you diagnose network problems
- → Because you have that visibility, the problems are fixed faster
- → Fewer interruptions to service and, therefore, your business

Data Based Predictions

- → Make more intelligent choices with more information (data) and access to historical data visibility that spans time – use patterns to anticipate network behavior

Greater Employee Efficiency

- → Enhanced visibility requires less investigation from engineers on the troubleshooting and resolution side, leaving more time for forward-moving company initiatives



Blind Spot Removal: 6 Approaches

These methods will help you monitor and troubleshoot your network's digital transformation initiatives and maintain success in daily operations.

01 Network Monitoring

Network monitoring tools validate if policies are working as planned and assist in tracking network performance and health. Some offerings do one or the other. Ideally, you can find one that does both.

- **Packet Capture** - Packet capture, also known as packet analysis or PCAP sniffing, captures and live packet data from Layers 2-7, traveling across your network. It uses TAPS and Port Mirroring, also known as SPAN, to do this. Packet capture is preferred for granular troubleshooting because it can identify the root cause of network issues. Packet Capture can bring visibility to challenging areas like WiFi connections, data centers, and remote sites.
- **Flow Monitoring** - Flow analysis enabled devices like routers and switches to generate flow data from their IP traffic. This IP-based method provides a high-level summary of network health. Flow monitoring is excellent for observing distributed WAN and SD-WAN links.
  - → Flow monitoring also shines a light on network threats. Traffic spikes and peaks in bandwidth usage can indicate a DDoS. Using flow analysis, you can find the IP source from where the malicious traffic originates.

Packet and Flow Network monitoring tools that unite packet and flow monitoring help close blind spots during deployments from the network core to cloud infrastructure.

Blind Spot Removal: 6 Approaches

02 Device Managed Services

Keep track of all devices used on the network with a cloud-based device inventory platform. Device-managed services show who is responsible for what devices, where they are located, and their status. With visibility into historic device performance, you gain a longer lead time before a device reaches its end of life (EOL).

03 Network Mapping

A topographical visual of the entire network, including remote sites, allows you to monitor WAN links and their dependencies and quickly spot any unusual network activity globally – determine which uplinks handle the highest quantity of traffic and how it flows between sites. See network performance from one dashboard – this lets you pinpoint problem areas in equipment or otherwise. Network mapping is helpful for SD-WAN management. You need to be able to see what paths your application traffic takes.

04 Alerting

Set up threshold notifications to see when a slowdown is happening and address any bottlenecks in traffic or when approaching capacity limits.

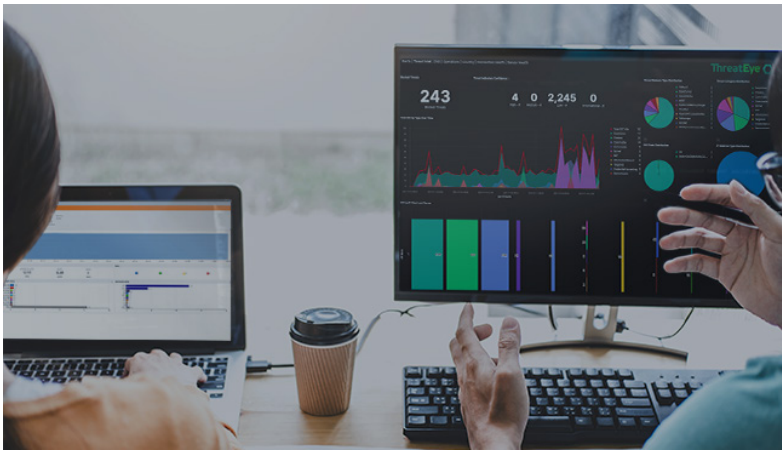
Setting network notifications for when traffic hits specific metrics gives you immediate feedback on network concerns before conditions worsen. Alerts on increasing latency give NetOps time to respond and remediate before a crash.

05 Encrypted Traffic Analysis (ETA)

Encrypted traffic analysis reveals if the content of the SSL/TLS traffic passing across a network has malicious indicators. This method is preferred over decryption. Decryption is bandwidth-intensive and often impacts network performance. On the other hand, ETA uses AI and ML from packet metadata to identify malicious traffic without disrupting network traffic.

06 User Authentication

Authenticating the users accessing the network helps with edge blind spots. Authentication is the easiest safeguard against blind spots when dealing with end-users and undiscovered devices. Although 2FA (2-factor authentication) is widely used, today's most secure standard is MFA (multifactor authentication) which requires three identity confirmation checks or a biometric fingerprint or face scan to access the network.



Risk for Leaving Blind Spots in Place

Leaving a network visibility strategy out of operational planning can save an organization pennies but lose them dollars.

Interrupted connections, poor application performance, and network outages lead to financial loss that significantly outweighs any initial cost of network monitoring and detection tools. Here are how some of those costs take shape:

Lost business opportunity

- A decline in employee productivity from spotty network availability
- Diminished employee morale from unreliable access to tools they need and systems going down
- Prospects who lose interest from interrupted demos, meetings, or choppy phone calls that come across as red flags

Damaged reputation and credibility

- Tickets and requests go unanswered during outages creating the impression of unresponsiveness.
- Customers are negatively impacted during outages and question if your company has the resources to support your product.

LiveAction is a platform of next-generation tools purpose-built to maximize network visibility and erase your blind spots.

Here's how:

Encryption Blindness:

- **ThreatEye NV** - ThreatEye's Deep Packet Dynamics (DPD) scans for packet traits and behaviors to fingerprint traffic for threat profiles without using resource-intensive decryption.

Network Blindness:

- **Packet Capture** – Omnipeek, the world's most powerful protocol analyzer, LiveCapture, our enterprise packet capture solution that can handle 100G networks, and LiveWire, our solution to extend visibility to the WAN edge, work in conjunction as packet protocol analyzers
- **NetFlow monitoring** – LiveNX tracks NetFlow from network devices and integrates with LiveWire's packet analysis for unified reporting and visualization

Edge Blindness:

- LiveAction includes a DMS cloud platform that logs devices for LiveWire and ThreatEye NV appliances for easy configuration, reset, and troubleshooting.
- Track and monitor hard-to-reach places, troubleshoot VoIP calls, and map network topography with LiveWire nodes.

Event Blindness

- Set advanced targeted alerting for custom audiences and at desired thresholds and intervals to avoid "over alerting fatigue."

Visibility Blindness

- Visually rich topographical network monitoring unites our packet capture and NetFlow analysis products within one interactive dashboard for easy reporting.

Don't settle for managing a network with one eye shut. Choose a platform that can do it all. Get visibility into TDR, APM, and NPM stats from every side. Get the broadest telemetry platform available on the market. Get LiveAction.

LiveAction®

960 San Antonio Rd, Suite 200, Palo Alto, CA 94303
+1 (888) 881-1116

About LiveAction

LiveAction provides end-to-end visibility of network and application performance from a single dashboard. This gives enterprises confidence that the network is meeting business objectives, offers IT administrators full visibility for better decision making, and reduces the overall cost of operations. By unifying and simplifying the collection, correlation, and presentation of application and network data, LiveAction empowers network professionals to proactively and quickly identify, troubleshoot, and resolve issues across increasingly large and complex networks. To learn more and see how LiveAction delivers unmatched network visibility visit **www.liveaction.com**.