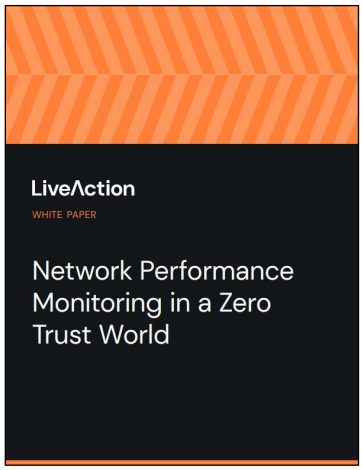
LiveAction

carahsoft.



Network Performance Monitoring in a Zero Trust World

Thank you for downloading this LiveAction white paper. Carahsoft is the reseller for LiveAction network performance solutions available via NASA SEWP V, RCA - Orange County – OMNIA Partners, Educational Software Solutions and Services – OMNIA Partners, Public Sector, and other contract vehicles.

To learn how to take the next step toward acquiring LiveAction's solutions, please check out the following resources and information:

For additional resources:
carah.io/liveactionresources

For upcoming events:
carah.io/liveactionevents

For additional LiveAction solutions:
carah.io/liveactionsolutions

For additional Network Visibility solutions:
carah.io/liveactionsolutions

To set up a meeting:
LiveAction@carahsoft.com
888-662-2724

To purchase, check out the contract vehicles available for procurement:
carah.io/liveactioncontracts

For more information, contact Carahsoft or our reseller partners:
LiveAction@carahsoft.com | 888-662-2724

LiveAction

WHITE PAPER

Network Performance Monitoring in a Zero Trust World

Executive Summary

In an era of evolving cyber threats and the increasing complexity of government networks, the adoption of a Zero Trust security model is gaining prominence in the federal space. Zero Trust challenges the traditional security paradigm by assuming that threats can emerge from both external and internal sources.

Executive Order 14028, OMB's M-21-31, and NIST SP 800-207 have been driving forces behind the federal government's rapid adoption of Zero Trust.

Never Trust, Always Verify

Zero Trust is a modern security model founded on the design principle "Never trust, always verify." It requires all devices and users, regardless of whether they are inside or outside an organization's network, to be authenticated, authorized, and regularly validated before being granted access.

With the rise of remote work, bring your own device (BYOD), and cloud-based assets that aren't located within an enterprise-owned network boundary, traditional perimeter security falls short. That's where Zero Trust comes in. A Zero Trust architecture (ZTA) is designed as if there is no traditional network edge, retiring the old castle-and-moat model of perimeter security.

Zero Trust Network Intelligence

Visibility is the foundation of zero trust; you can't protect what you don't know. This is where LiveAction's network intelligence platform comes into play. Network intelligence plays a crucial role in supporting Zero Trust security in the federal space by providing these key benefits:

01 Continuous Visibility

LiveAction's platform offers real-time visibility into network traffic, allowing Federal agencies to monitor user and device activities continuously. This visibility is crucial for implementing the "never trust, always verify" principle of Zero Trust.

02 Anomaly Detection

Identify unusual patterns or behaviors within the network. This is essential for detecting potential security threats or deviations from normal network behavior, aligning with Zero Trust's emphasis on continuous monitoring.

03 Micro-Segmentation Monitoring

Granular visibility into traffic within segmented zones. This capability enables organizations to monitor and control communications at a detailed level, supporting the micro-segmentation approach often associated with Zero Trust.

04 User and Device Authentication Integration

Integration with identity management systems and user authentication processes is critical for Zero Trust. LiveAction supports such integrations and can help enhance the verification process and ensure that only authorized entities gain access to the network.

05 Policy Enforcement

The platform can assist in enforcing access policies by monitoring network traffic to ensure compliance with the principle of least privilege. This helps organizations prevent users from exceeding their authorized access levels.

06 Traffic Analysis and Reporting

Detailed traffic analysis and reporting capabilities provided by LiveAction's visualization and reporting engine are essential for understanding network activities. This is valuable for implementing and enforcing access policies based on the principle of least privilege in a Zero Trust architecture.

07 Encrypted Traffic Analysis

LiveAction's platform supports the inspection of encrypted traffic by using Deep Packet Dynamics (DPD), a highly effective, non-invasive method, that allows admins to profile traffic characteristics and anomalies for risk without requiring decryption. This aligns with the heightened use of encryption in Zero Trust architectures.

08 Advanced Behavioral Analysis

Leverage an AI-powered analysis engine, combining data collection, advanced behavioral analysis, predictive threat intelligence, and machine learning to detect threat actors and comply with security regulations.

09 Response and Remediation

Quickly respond to security incidents. LiveAction's platform can trace the source of anomalies, understand the extent of incidents, and facilitate remediation measures promptly.

10 Cloud and Edge Monitoring

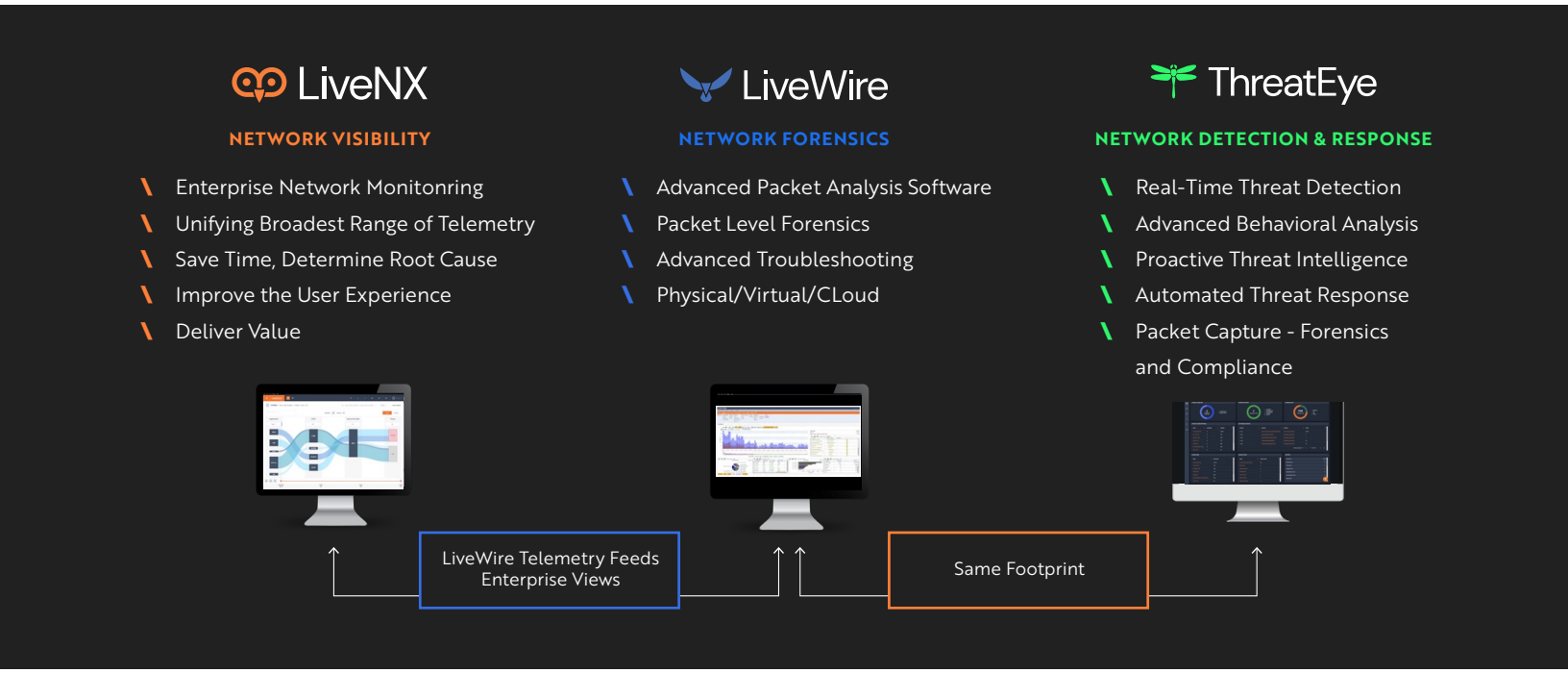
Extend monitoring capabilities to cloud and edge environments, helping to ensure that Zero Trust principles are applied consistently across all parts of the network infrastructure, including those outside traditional data centers.

11 Scalability and Flexibilty

Federal networks are complex and constantly evolving, and LiveAction's platform supports high levels of flexibility and scalability. This ensures that the platform can adapt to changes in network architecture and support the growth of the organization's infrastructure.

LiveAction's Network Intelligence Platform

LiveAction offers solutions for network performance monitoring (LiveNX), packet capture and forensic analysis (LiveWire), and network detection and response (ThreatEye). In short, LiveAction delivers real-time network intelligence to monitor, troubleshoot, and help secure enterprise networks and applications no matter where they are, including on-premises, hybrid, SD-WAN, and cloud operations.



Conclusion

By adopting a robust and Zero Trust-aware NPM approach, federal agencies can gain valuable insights and improve their overall security posture. Network performance monitoring becomes a proactive tool, not just for ensuring optimal network health, but also for actively contributing to a strong and dynamic Zero Trust security architecture.

To learn more about how LiveAction's Network Performance Monitoring solution helps to streamline and simplify network management for companies looking to optimize their network operations, please **Contact Us**.

Additional Resources

- OMB M-21-31: How LiveAction Supports the US Federal Government
- Accelerate Your Journey to Zero Trust

LiveAction

901 Campisi Way, Suite 222
Campbell, CA 95008
(888) 881-1116

LiveAction provides end-to-end visibility for network security and performance. By relying on a single source of truth – the packets – LiveAction gives modern enterprises the confidence needed to ensure the network is securely meeting business objectives, providing full network visibility to better inform NetOps and SecOps, and reducing the overall cost of network and security operations. By unifying and simplifying the source of collection, inspection, presentation, and analysis of network traffic, LiveAction empowers network and security professionals to proactively and quickly identify, troubleshoot, and resolve issues across increasingly large and complex networks.

To learn more about LiveAction, visit www.liveaction.com