White Paper

swish | riverbed

Enabling the Connected Warfighter

Are today's connected warfighters able to reliably and consistently login, communicate, access data, gain competitive insights, and take action at the speed of relevance?

Introduction

Enabling the Warfighter

As the vision of the Joint All Domain Command and Control (JADC2); Joint Information Environment (JIE); and other Defense Shared Services are adopted, the complexity and dependencies upon the end-to-end architecture's performance increases exponentially. Delivering an information advantage at the speed of relevance is critical. More than ever, speed of improvements and innovation matter.

Tactically, JADC2's three guiding principles are 'sense,' 'make sense,' and 'act.' The intent is to produce a warfighting capability to act at all levels and phases, across all domains, with partners, to deliver information advantage at the speed of relevance.

Artificial intelligence, machine learning, and automation can deliver amazing advantages. However, mission decisions and execution still ultimately depend on our warfighter. Their ability to reliably and quickly login, communicate, access data, gain competitive insights, and take action must be seamless.

"IT is the foundation of our competitive advantage" - Lauren Knausenberger, CIO, US Air Force. Air Force Magazine, "'Fix my computer' Cry Echos on Social Media; Air Force CIO Responds," Jan. 26, 2022, by Shaun Waterman.

In today's digital world, speed of relevance is tightly coupled with IT end-to-end performance.

Why Warfighter Experience Matters

Somewhere overseas, unmanned aerial vehicles (UAVs) are flying over a small peninsula collecting real-time intelligence. The UAVs continually transmit crucial intelligence to a regional Combatant Command. The Combatant Command integrates the intelligence into the Common Operating Picture (COP). A Marine Expeditionary Unit (MEU) deployed on Navy ships off the coast of the peninsula uses the timely intelligence to inform their Amphibious Landing mission. Minutes later a thousand Marines deploy from the ships with up-to-the-minute insights.

In this and many other real-life scenarios, warfighters rely on high-quality end-to-end system performance to make insightful decisions at the speed of relevance. If a device is slow, a network is down or data is not available, the mission is at risk.

DOD leadership recognizes these dependencies and has assigned Levels of Effort (LOEs) to establish the JADC2 **Human, Data,** and **Technical** Enterprises. JADC2's Guiding Principles speak to warfighter experience, calling out needs for (1) improvements at the enterprise level, (2) data fabric efficiencies and evolvability, (3) resiliency, (4) unified development and implementation, and (5) execution at faster speeds.

As missions become more reliant on data-driven decisions, warfighter lives increasingly rely upon digital performance. Warfighter digital experience matters more than ever before.

Defining Warfighter Experience

At the simplest level warfighters need a fast, predictable experience when they login to their computers and access applications to execute their missions. Within DOD's end-to-end IT architecture, many diverse technology components depend on each other to deliver a quality experience. For a quality digital experience each individual component in the system must provide adequate capacity, latency and error-free quality.

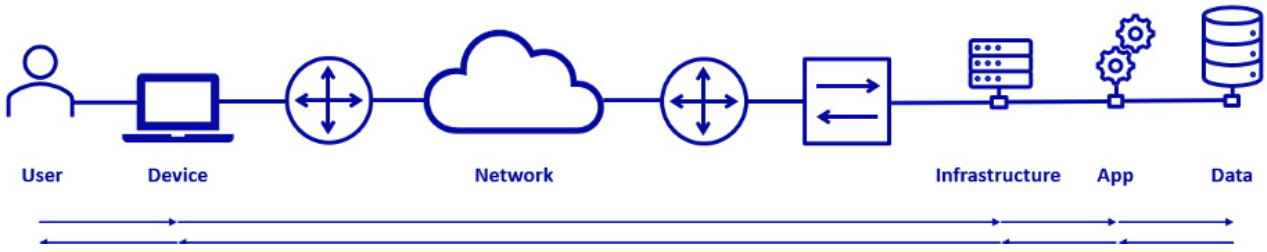

Figure 1 - Example DoD End-to-End IT Architecture

US Government executive leadership recognizes how critical user experiences are for mission success. The *President's Management Agenda Priority 2 (Excellent Experience), the 21st Century Integrated Digital Experience Act,* and the *US Digital Service Performance Guidelines* all provide guidance regarding why user experience matters and how to measure user experience with continuous qualitative and quantitative analysis.

To successfully enable warfighter experience in a digital world and continuously innovate, much like with JADC2, our DOD IT teams must be able to collectively 'sense', 'make sense' and 'act' in respect to their cyber domains.

CHALLENGE TO WARFIGHTER EXPERIENCE

In August 2020, General Charles Q. Brown, Jr., Chief of Staff for USAF, published "Accelerate Change or Lose." In this eight-page document the General states, *"If we don't change – if we fail to adapt – we risk losing the certainty with which we have defended our national interests for decades. We risk losing a high-end fight. We risk losing quality Airmen, our credibility, and our ability to secure our future. We must move with a purpose – we must Accelerate Change or Lose."*

However, DoD struggles with delivering quality digital warfighter experiences.

In January 2022, a widely shared post on LinkedIn indicated severe user frustration. Michael Kanaan, the director of operations for the Air Force's Artificial Intelligence Accelerator at MIT, posted, *"you tell us to 'accelerate change or lose,' then fix our computers."* Although employed by the USAF, Mr. Kanaan's post was directed to the DoD, *"before you buy another plane, tank or ship, fix our computers. Yesterday I spent an hour waiting to log-on."*

In a Defense One interview in Oct 2019, Colt Whittall, the Air Force's first Chief Experience Office (CXO) was quoted as saying *"When you go out and talk to the airmen and ask, "What's working and what's not when it comes to IT?" … they have the same hot button about the network, broadly defined. But they will also tell you about difficulties they have with a wide variety of software applications…with a difficult user experience."*

In April 2022 during an AFCEA TechNet Cyber presentation, Lt. General Robert Skinner, DISA Director, boldly stated, *"wouldn't it be cool if… end point performance didn't crush souls."*

Warfighters across the globe suffer productivity loss and frustration due to horrible digital experiences. Leaders are keenly aware of the challenges. What can we do to better enable our warfighter experience?

COMPLEXITIES OF DOD INFORMATION NETWORK AND JADC2

Operating, troubleshooting, and improving the end-to-end DOD IT architecture is extremely complex. Figure 7 outlines the many components which depend on each other to complete a common user transaction. The components of this end-to-end system are managed by disparate IT teams, which complicates operating it successfully 100% of the time.

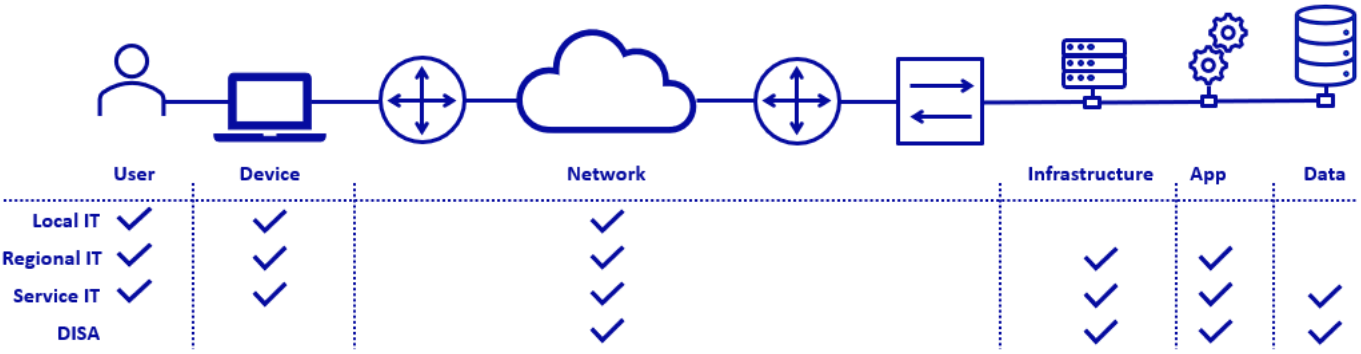

Figure 2 - Example DoD End-to-End IT Architecture

Using legacy approaches with siloed tools, poor cross-departmental communications, and a lack of insight into warfighter experience won't suffice as the DoD increasingly relies on technology for information dominance and speed of relevance.

SILOS LEADS TO LOW PERFORMANCE

Commercial enterprises recognize how important teamwork and end-to-end digital operations are to competing in today's rapidly evolving global landscape.

"The conversation around IT operations has evolved and operations now support more complex distributed systems with many architectures, integrations, and dependencies. The unpredictability of these systems requires new automated detection, observability, and healing." – Gartner®, Hype Cycle™ for Monitoring, Observability and Cloud Operations, 2021 Padraig Byrne and Pankaj Prasad.

Silos lead to compromised teamwork, lack of cooperation, and a weak digital foundation for digital mission success.

While modern IT teams have more data than ever before, this data is often siloed and provides no unified context or actionable insights. IT teams are being overwhelmed with alerts that are essentially noise because they lack unified context or intelligent investigative insights. Without broader context on which alerts have the largest impact, IT teams can easily get bogged down in troubleshooting inconsequential events.

In many cases, IT teams have difficulty triaging alerts across domains and end up pulling in experts to solve low-level tech issues because it's difficult to determine the difference between high and low priority alerts. This means highly skilled specialists get pulled away from mission-critical work they should be focused on. Unfortunately, without AI/ML enhanced end-to-end investigations the largest teams can't possibly maintain pace while using manual human analysis to complete complex end-to-end troubleshooting.

Legacy monitoring tools have additional shortfalls. They limit or sample data, which can frustrate IT teams by making it difficult to proactively identify potential issues and opportunities for improvement. After all, how can IT teams be expected to consistently — and correctly — solve problems if they can't contextually 'make sense' of the end-to-end environment due to missing data?

Additionally, troubleshooting complex issues with siloed, domain-specific tools requires war rooms, manual investigation, and manual correlation by IT experts whose skills are scarce and difficult to replicate. To be effective in today's fast-paced world organizations need a better approach to ensuring digital service quality and effective collaboration in complex distributed environments.

TEAR DOWN SILOS

Industry research is clear, when teams tear down silos, trust each other, and collaborate with mutual respect they deliver amazing results. This stands true within DOD at SOCOM, it's proven in the airline industry with Crew Resource Management (CRM) training to improve flight safety, and it's being accomplished in the technology sector by DevOps and Site Reliability Engineering (SRE) teams who deliver thousands of improvements per day at high rates of success.

Generative teams with high trust, strong collaboration, empathy, and willingness to innovate **significantly outperform** bureaucratic siloed teams with low trust, poor collaboration, scapegoating, and adversity to change. *The State of DevOps 2021* report found elite performers significantly outperformed lower performances in key operational metrics by huge margins.

"Efficiency remains important, but the ability to adapt to complexity and continual change has become an imperative."
– Retired U.S. Army General Stanley McChrystal, *"Team of Teams: New Rules of Engagement for a Complex World"*

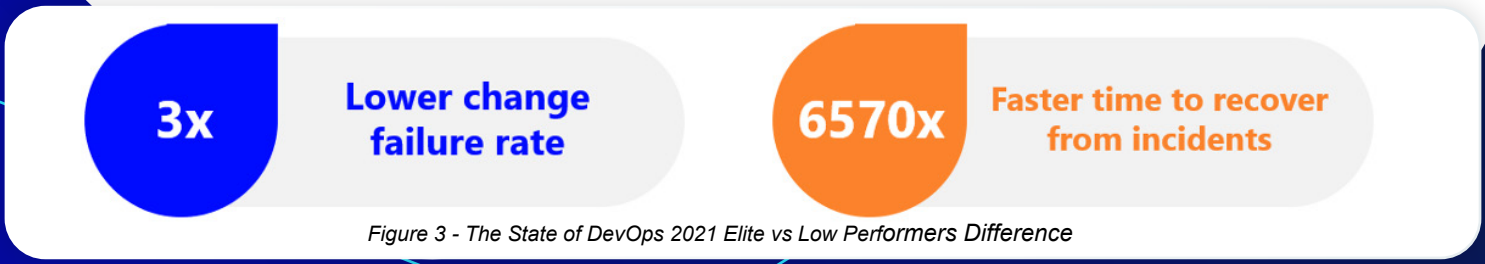

Figure 3 - The State of DevOps 2021 Elite vs Low Performers Difference

UNIFIED OBSERVABILITY POWERED BY ALLUVIO

When organizations invest in an observability platform that unifies data, insights, and actions across IT, they can eliminate data silos, resource intensive war rooms, and alert fatigue. They can enable faster, more effective decision-making across domains, apply expert knowledge more broadly, and continuously improve warfighter experience.

When tools limit or sample data, IT may not even be aware of other potential issues or opportunities for proactive improvement. Observability is meant to solve these problems, but current solutions fall short. Even so-called "full-stack" observability solutions fail to capture all relevant telemetry and sample data to deal with the scale of today's distributed environment. Most solutions only collect three or four types of data and are limited to DevOps, Site Reliability Engineers, or cloud-native use cases. And they offer nothing beyond the alert, so IT still relies on their resident experts to manually investigate events.

Riverbed has a different and superior vision for observability. Alluvio Unified Observability unifies data, insights and actions at mission speed, empowering all IT teams to deliver seamless digital experiences and end-to-end performance.

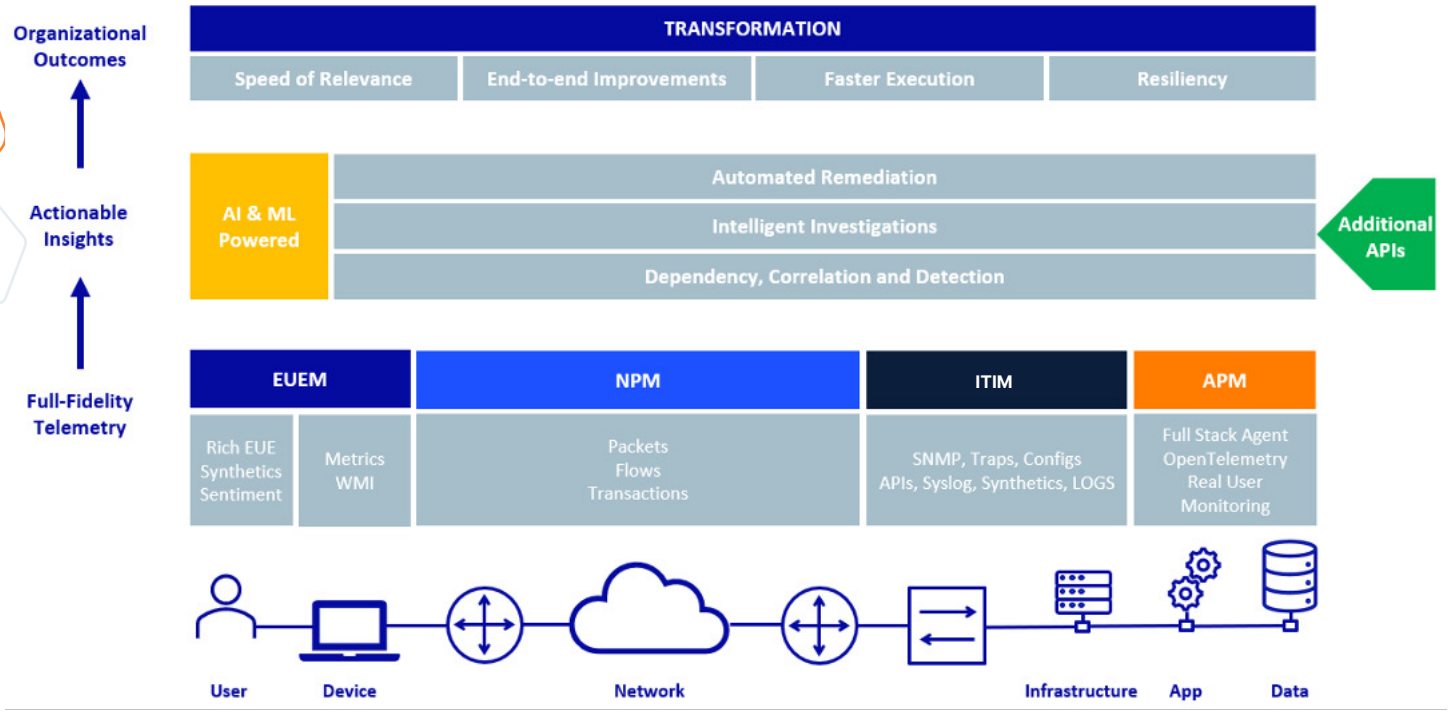

Figure 4 - Alluvio Unified Observability

UNIFIED DATA – 'SENSE'

Alluvio Unified Observability captures full-fidelity data across diverse sources (users, devices, networks, servers, applications, cloud-native environments, and third-party feeds) for a complete view of IT performance. Unlike other solutions that sample data to deal with the scale of today's distributed environments, Alluvio analyzes every transaction, packet, and flow, as well as the actual user experience for every type of application.

Full-fidelity data gives IT teams a complete 'common operating picture' of what's happening and what has happened, without missing key events due to sampling. Full-fidelity data is available for all the various IT teams so they can work together and understand the end-to-end context of the digital landscape.

Full-fidelity data types range from simple metrics to rich multi-dimensional telemetry to detailed packet captures.

TYPES OF FULL FIDELITY DATA CAPTURED BY ALLUVIO

Metrics are scalar values collected to represent system state at a point in time and are of low cardinality. Examples of metrics include CPU utilization, disk IOPs, average bits per second, percent of utilization, queue drops, and other one-dimensional measurements sourced from Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), cloud infrastructure APIs, and similar methods.

Multi-dimensional telemetry are structured records with extensive details and are of high cardinality. This allows flexible analysis of the aggregate data from many points of interest while still enabling drill down to individual transactions. Example data points in multi-dimensional telemetry include, but are not limited to, source, target, start time, stop time, load, latency, error codes, paths, queries, and additional contextual metadata. Multi-dimensional telemetry often comes from an open-source agent such as OpenTelemetry; cloud APIs; proprietary solutions such as Alluvio Aternity, Alluvio NetProfiler, Alluvia AppResponse; and similar methods or sources.

Packet captures provide deep forensic details into what was exactly sent over the network at a specific point. This robust information is critical for many complex troubleshooting processes when different points in the environment need to be observed and compared to determine what happened along the path. For DOD organizations, having packet captures near the user at the edge, and at the core near the application, can be extremely useful in determining if something along the network caused an issue.

High cardinality and rich details matter for observability. High cardinality of performance data across a breadth of observation points for utilization, latency, and errors is very useful at identifying insights for troubleshooting a system when using AI/ML methodologies.

Alluvio's ability to 'sense' full-fidelity performance data along the complete DODIN and JADC2 paths enable the broadest set IT teams to collectively gain rich data points with a consolidated solution – instead of siloed tools.

UNIFIED INSIGHTS – 'MAKE SENSE'

While other solutions correlate disparate events and alerts based primarily on time or require lengthy asset database integrations, Alluvio automates the process of gathering and correlating measurements from various domains to provide unified, context-rich, filtered, and prioritized insights that help all IT teams understand the scope and severity of issues and the cause of poor performance. Alluvio's full-fidelity data across IT domains empowers AI/ML workflows to 'make sense' of the data based on each IT team's contextual needs. Furthermore, Alluvio allows various IT teams to collaborate with each other instead of 'point fingers'.

The DODIN and JADC2 are highly distributed systems of massive scale. The complexity of monitoring and troubleshooting a distributed system with extreme points of dependency is not humanly possible. Alluvio's AI/ML algorithms analyze millions and billions of dependences using specialized deterministic AI and highly tuned ML approaches to find common and never-before-seen performance issues. With actionable context-rich insights, warfighter experience issues such as slow device startup, long login times, device crashes, Microsoft Teams failures, network congestion, slow web performance, or application errors, all become easily triaged to the proper team for rapid action. Alluvio allows IT staff to focus their valuable time on acting on the intelligence, instead of spending hours or days attempting to manually dig through 1,000,000+ data points across multiple IT domains to find the 1% of telemetry related to the root cause.

Through open APIs, these actionable insights bring value to the broader IT Service Management ecosystem of tools within the DOD.

UNIFIED REMEDIATION – 'ACT'

Alluvio Unified Observability includes an expandable library of pre-configured and customizable actions to support manual remediation and automated self-healing of common issues. Remediation actions are recommended by the system based on the issue being investigated, but IT maintains decision making control on whether and when to execute the suggested corrective action.

For example, if an application running in a Kubernetes container experiences many HTTP 500 errors traced back to a failed process, Alluvio can execute a script to restart a new container and stop the failing container.

By unifying automated actions across IT teams, the DOD can improve teamwork, increase workforce efficiency, accelerate problem-solving, greatly improve warfighter satisfaction, and avoid stressful war rooms.

Riverbed Alluvio Unified Observability empowers DOD IT teams to apply JADC2's guiding principles of 'sense', 'make sense' and 'act' to their critical IT missions, which broader multi-domain operations and dominance rely upon.

OBSERVABILITY SELF-ASSESSMENT

This Observability Self-Assessment exercise below makes it easy to analyze your organization's ability to 'sense,' 'make sense' and 'act' in relation to your IT teams and digital mission capabilities.

QUALITATIVE CAPABILITIES

Answer the below questions "yes" or" no."

1. Can you understand what a specific warfighter's digital experience is at any given time?
2. Can you compare performance attributes from arbitrary groups of warfighters?
3. If your command's Executive Officer complained of application problems, could you isolate problems and understand why they were occurring?
4. Can you quickly (within minutes) isolate any fault in your system, no matter how complex?

TECHNICAL CAPABILITIES

In the table below rate each individual observability 'capability' from 0 (no capability) to 5 (cutting edge capability) by 'pillar.' In the bottom row total the score for each 'pillar' and then compute your total score by adding the pillar scores together. Identify and analyze your organization's weaknesses by pillar and capability.

	User (Warfighters)	Devices	Networks	Infrastructure (Services, OSs, Hypervisions & Containers)	Applications	Database, Warehouse & Lakes
Capacity Metrics						
Latency Metrics						
Error / Quality Metrics						
Multi-Dimnsional Telemetry						
Accross Environments (Clouds, Enclaves, etc)						
Accesible to All Teams						
Centrally Unified Data Set						
Scriptured Investigations						
Automated Remediation						
Total Score:						

LIST YOUR TOP THREE PRIORITIES FOR IMPROVEMENT:

1.

2.

3.

Once you have completed your self-assessment, contact Swish (info@swishdata.com or 888-460-0275) to schedule a discussion with an Observability Subject Matter Expert. Swish and Riverbed engineers have extensive experience with observability methodologies and technologies, as well as various defense programs of record such as DISA STEP/Teleport, Army WIN-T, SOF Deployable Nodes, Navy ADNS, Navy NMCI, Air Force airborne platforms, and other unique environments.

Swish is a Service-Disabled Veteran-owned and HUBZone certified small business provider of technology solutions and engineering services to the U.S. Federal Government with a focus on high-quality outcomes for our clients. Swish's focused Practice areas include Cybersecurity, Performance Engineering, IT Modernization and DevSecOps.

To learn more, please visit:
www.swishdata.com

1420 Spring Hill Road Suite 230 McLean, VA 22102

P 703.635.3324 / **E** info@Swish.com

swish | riverbed