



# TechNet Augusta

August 14–17, 2023 | Augusta Marriott at the Convention Center | Augusta, GA

## 2023 SOLUTIONS SHOWCASE





# AFCEA TechNet Augusta 2023 Solutions Review

## Enabling a Data-Centric Army

The U.S. Army's ambitious data plan released last fall provides the principles, goals and guidance needed to transform into the data-centric Army of the future. It establishes a foundation to enhance decision-making efficiency and effectiveness at every echelon and aims to improve interoperability among the sister services and with coalition and mission partners.

Varied and isolated data sources, where they still exist, limit data sharing, hamper decision-making and constrain cloud-computing capabilities, including artificial intelligence and machine learning. Evolving toward data-centricity requires the Army to unleash the full power of information across all mission areas and share across the military services and the entire Defense Department, enabling joint all-domain command and control (JADC2), allowing technical dominance and ensuring operational advantage over the peer and near-peer adversaries.

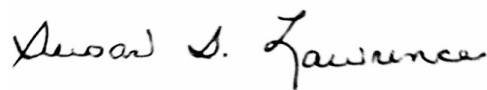
The Army Cyber Center of Excellence sought solutions to address emerging and existing challenges. Dozens of abstracts address the Problem Statements. This Solutions Review Compendium complements the event and helps build engagement.

The abstracts cover many complex challenges the Army faces. The Solutions Review offers industry the opportunity to engage and respond to pressing problems. Companies were invited to offer solutions to the following areas:

1. Bandwidth Limitations
2. Hybrid Cloud Solutions
3. Converged Assured Voice Communications
4. Converged Data Transport
5. Tactical Edge
6. Dynamic Spectrum
7. How do we use technology to correlate data and information to inform the commander of developing risks and opportunities to ongoing missions to enable timely decision making?
8. How do we use technology to provide a cyberspace social layer which correlates and identifies actors, units/individuals, their activities and organizational affiliation in the Common Operating Picture (COP) and Military Decision-Making Process (MDMP) products?

This digital transformation is a whole-of-Army effort with leaders across the service working diligently together and with the science and technology community and businesses large and small to gain data superiority on the digital battlefield and ultimately outmatch formidable competitors such as China, Russia and North Korea.

Best wishes,



**Lt. Gen. Susan S. Lawrence, USA (Ret.)**  
President and CEO  
AFCEA International

# Problem Statements

## Problem Statements from ACM Networks and Services

### Problem Statement 1

**Title:** Bandwidth Limitations

**Problem Statement:** Bandwidth limitations significantly hinder our ability to push, receive and analyze information at the tactical edge; how does your technology address this issue?

### Problem Statement 2

**Title:** Hybrid Cloud Solutions

**Problem Statement:** What are the benefits realized using your technology to facilitate the implementation of a hybrid cloud solution from the cloud provider (Army or Commercial) to the tactical edge?

## Problem Statements from ACM Tactical Radios

### Problem Statement 3

**Title:** Converged Assured Voice Communications

**Problem Statement:** What is the most operationally effective and non-cost prohibitive technology to provide secure communications components of converged C5ISR/EW systems to pass verbal information that enables tactical unit leaders as part of the Division as a unit of action in Army 2040?

### Problem Statement 4

**Title:** Converged Data Transport

**Problem Statement:** What is the most operationally and non-cost prohibitive technology to provide secure communications components of converged C5ISR/EW systems that directly enable machine to machine data exchanges for systems as part of the Division as a unit of action in Army 2040?

## Problem Statements from ACM Electronic Warfare

### Problem Statement 5

**Title:** Tactical Edge

**Problem Statement:** What small form factor (tactical edge) industry capability can perform AI/ML/ cognitive weaponizing (effects generation) for EW using ES operational information?

### Problem Statement 6

**Title:** Dynamic Spectrum

**Problem Statement:** What available technologies enable Army implementation of Dynamic Spectrum Access/ management technology for Army EMS-dependent capabilities at machine speed in an EMS contested and congested environment?

## Problem Statements from ACM Electronic Warfare

### Problem Statement 7

**Problem Statement:** How do we use technology to correlate data and information to inform the commander of developing risks and opportunities to ongoing missions to enable timely decision making?

### Problem Statement 8

**Problem Statement:** How do we use technology to provide a cyberspace social layer which correlates and identifies actors, units/individuals, their activities and organizational affiliation in the Common Operating Picture (COP) and Military Decision-Making Process (MDMP) products?

# Table of Contents

Accelerate Hybrid Cloud to the Edge with ICAM-on-the-Move Andrew Whelchel, Senior Solutions Engineer, Saviynt .....	11
Data Superiority at the Tactical Edge Baron Rawlins, Lead Solutions Architect, AWS .....	13
Solving Bandwidth Limitations at the Tactical Edge by Using Dejero’s Smart Blending Technology Bogdan Frusina, Founder, Dejero .....	14
Hybrid Cloud in a Tactical World Brendan Kelly, Data Protection Specialist, Dell.....	15
Enhancing Time-Based Analysis in Splunk Enterprise Security for Army Cyber Protection Teams Brent Matlock, Senior Consulting Solutions Engineer, Splunk .....	16
Virtual Mobility at the Edge: Full Garrison Capabilities Using a Fraction of the Bandwidth Brian T. Kovalski, Senior Vice President, Federal, Hypori .....	17
Virtual Mobility at the Edge: Gain Cross-Domain Access from a Single Device Brian T. Kovalski, Senior Vice President, Federal, Hypori .....	18
The Future of Virtual Mobility at the Edge: Enabling Secure Comms with Command-and-Control Networks at Any Level Brian T. Kovalski, Senior Vice President, Federal, Hypori .....	19
Enabling JADC2 Through Secure Data Security Chris Brown, Public Sector Chief Technology Officer, Immuta .....	20
Leveraging Cloud Computing to Overcome Bandwidth Limitations at the Tactical Edge Chris Ernst, Senior Solutions Architect, AWS .....	21
Hybrid Cloud Solutions Chris Ernst, Senior Solutions Architect, AWS .....	22
Meeting the Need to Rapidly and Reliably Collect and Convert Messy Data and Signals into Actionable Intelligence Christopher Stephenson, Head of AI Operations, Nuix .....	23

Focusing on Data Without Ignoring Voice Communications	
Courtney Stiles, Director of Business Development, REDCOM Laboratories, Inc. ....	26
Operationally Effective and Non-Cost Prohibitive Technology to Provide Secure Communications Components of Converged C5ISR/EW Systems	
Courtney Stiles, Director of Business Development, REDCOM Laboratories, Inc. ....	27
Enabling Hybrid Cloud With Cloud Ready Networks	
Craig Hill, Distinguished Architect, U.S. Public Sector – CTO, Cisco .....	28
Leveraging Neuromorphic Technology in Today’s Battleground and Turning Raw Data into Actionable Information for Commanders at the Edge!	
Jason K. Dunn-Potter, Solutions Architect & Mission Specialist, Intel .....	30
How Intel is Building Hybrid Clouds to Maximize Operations	
Jason K. Dunn-Potter, Solutions Architect & Mission Specialist, Intel .....	32
Data Approaches to Improve Mission Effectiveness	
Dr. Paul Lieber, Chief Data Scientist, Peraton .....	34
Hybrid Cloud Solutions – A Bridged Approach	
Dr. Paul Lieber, Chief Data Scientist, Peraton .....	36
Data Protection at the Edge	
Gina Scinta, Deputy Chief Technology Officer, Thales TCT .....	38
Protecting Your Data in Their Cloud	
Gina Scinta, Deputy Chief Technology Officer, Thales TCT .....	39
Hybrid Cloud Adoption on the Forward Edge of Battle	
Hansang Bae, Public Sector Chief Technology Officer, Zscaler .....	40
Digital Twins, Driven by a Secure COTS Cross Departmental Data Mesh, Advance Decision Making to the Speed of Relevance	
Jacques Jarman, CRO, Edge Technologies.....	41
The Ultimate Flexibility in Hybrid Data Management and Data Analytics	
James S. Herron, Solution Engineer, Cloudera Government Solutions, Inc. ....	43
I Got 99 Problems, but Compliance Ain’t One	
Joe Hagan, Senior Sales Engineer, Splunk .....	45

Protecting Hybrid, Multi-Cloud Environments	
John Harmon, RVP, Cyber Solutions, Elastic Federal Cyber Solutions.....	46
Multi-orbit, Multi-Link Terminal for Bandwidth Resiliency at the Tactical Edge	
John Lane, Chief Sales Engineer, ALL.SPACE.....	48
Bringing 5G Capacity, Capabilities to the Battlespace	
Ken Riordan, Principal Architect, Nokia Federal Solutions .....	50
Bringing 5G AI and Frequency Agile Cognition to the Tactical Edge	
Ken Riordan, Principal Architect, Nokia Federal Solutions .....	51
Hybrid Cloud Solutions — People, Process & Technology	
Kimberly C. Ullmann, Team Lead, Peraton .....	52
Providing Service Views for C2 Situational Awareness	
Lee D. Koepping, Chief Technologist, ScienceLogic .....	54
Achieving a Unified Hybrid Cloud Through Model-Driven DevOps	
Lee Van Ginkel, Team Leader - Federal Platforms and Automation, Cisco .....	56
Leveraging Army Investments in VMWare Technologies to Meet Target Level Zero Trust and the Path to Advanced ZT	
Leo Lebel, Senior Solutions Architect	
Chris Lewis, Sr. Account Executive, Network and Security, Federal	
James Emmons, Networking & Security Specialist Account Executive, VMware .....	58
NetApp ONTAP: A Simple, Flexible Solution for AI at the Edge as a Hybrid Cloud Solution	
Mario LaNasa, Senior Solutions Engineering Manager	
Matt Dawson, District Sales Manager, NetApp.....	60
Empowering the Edge with Event Streaming	
Michael Peacock, Staff Solutions Engineer, Confluent .....	62
Providing a High-Bandwidth, Low-Latency Symmetric Communications Solution	
Peter Ford, EVP, Government Operations, QuSecure.....	63
Helping the Army Create a Data Centric Fabric While Consolidating and Streamlining the Enterprise and Tactical Networks	
Rich Gleason, New Business Proposals, Huntington Ingalls Mission Technologies. ....	64



Leveraging Cisco Soft Client on ATAK with Cisco Communications Manager: An Abstract Response	
Robert Alred, Technical Solutions Architect, Cisco .....	65
Bandwidth Limitations	
Rohit Bhanot, Vice President, JMA Wireless .....	67
Tactical Data Operations	
Ron Nixon, CTO & CISO, Federal Organization, Cohesity .....	68
Heightened, Accelerated Performance at the Tactical Edge	
Russel Davis, Chief Operating Officer and Chief Product Officer, Vcinity, Inc. ....	69
Semantic Search & Sentiment Analysis (Se3An) — High-Definition Mapping of the Information Environment	
Stefano Feijoo, Data Scientist, Peraton .....	71
Firmware Under Fire? A Critical Gap in Cybersecurity Programs	
Stephen “Steve” Spry, Founder, Spry Squared, Inc.....	73
Leveraging Virtualization Combined With NSA-Vetted, Pre-Engineered, Scalable Hybrid Infrastructure to Achieve Secure and Flexible Operations	
Therman Farley, Vice President, Information Solutions Group, Trace Systems, Inc. ....	75
Meeting the Critical Need for a Compact, Secure, Versatile Tactical Edge Processing Capability	
Therman Farley, Vice President, Information Solutions Group, Trace Systems, Inc. ....	77
Identifying Non-CVE Risks Within OT & ICS	
Thomas Pace, Co-Founder & CEO, NetRise.....	78
Setting a Fast Path Toward Cloud Adoption	
Tommy Dammer, Senior Solutions Engineer, VMware .....	79
Project Fort Zero End-to-End Solution	
Will Robinson, Federal DoD Chief Strategist, Dell Technologies .....	80
Security-First AI	
Zach Vaughn, Director, Federal Security Engineering, Vectra AI.....	81
Operationalizing AI in Cyber: Creating Opportunities for Long-Term Strategic Advantage	
Zach Vaughn, Director, Federal Security Engineering, Vectra AI.....	82

# Submissions

# Accelerate Hybrid Cloud to the Edge with ICAM-on-the-Move

**Andrew Whelchel, Senior Solutions Engineer, Saviynt** • [andrew.whelchel@saviynt.com](mailto:andrew.whelchel@saviynt.com)

## ABSTRACT

The speed of change in the joint contested environment is moving at a breakneck rate. With the introduction of multi-domain and artificial intelligence (AI) assets, along with traditional mission systems, this creates the impetus to drive the cloud resources to tactical edge faster than ever before. With this speed come new risk challenges. Hybrid cloud assets bring to the commander, leader and soldier definitive options to mediate this risk of operating at the tactical edge and to meet the mission needs with success.

Key to success of hybrid cloud delivery is not just an identity solution in the form of ICAM, but more specifically, an ICAM-on-the-move capability that can meet the needs at the tactical edge. Fundamental to the ICAM solution operating at the edge is the ability to rapidly onboard and offboard digital assets using least privilege access to attributes to enable the hybrid cloud resources to operate at the edge. As part of this integrated capability, the ICAM-on-the-move enables rapid and secure zero-trust access to digital assets at the edge while minimizing risk to operate at the speed of the mission.

Enabling the hybrid cloud with ICAM-on-the-move addresses key challenges in multi-domain assets at the edge. Some of these challenges include rapid roll-on/shut down of assets, operating in disconnected environments, deploying new ML models to multi-domain assets and removing AI data access when needed for data disposition.

Delivering on these challenges requires a hybrid cloud enabled with ICAM-on-the-move identity capability that is accessible from cloud core to tactical edge. The ICAM-on-the-move enabled hybrid cloud brings capabilities to the joint theater including:

- Provide access authorization capability across the hybrid cloud to the tactical edge to drive rapid and secure access to resources.
- Enable strong zero-trust multi-factor authentication (including the use of certificates) with broad access from the hybrid cloud to local IdP when running disconnected operations.
- Provide secure data access authorization for edge AI and data analytics access enabling access to the command post and edge field environment.

ICAM-on-the-move enables rapid delivery of hybrid cloud secure access to the edge to support the joint multi-domain mission. The capabilities described here would include details of capabilities, technical architecture and use case scenarios to further enable the success of the mission.

**BIO:** Andrew Whelchel (CISSP-ISSAP, ISSEP, CAP, CCSP, CSSLP) started in information security and IAM immediately after graduation from the University of Memphis, supporting identity and access management managing Microsoft Identity for U.S. federal customers. Later work transitioned to network infrastructure security and then to consumer identity protection in the role at RSA Security and most recently at Okta and Saviynt. At RSA Security supporting financial services, health care, U.S. federal and other customers, there was focus on identity risk analytics and integration of identity fraud intelligence for cybercrime prevention. At a prior role at Okta and the current role at Saviynt, he is focused on protecting employees as well as business partner identities for public sector agencies to reduce cyber risk as well as accelerate capabilities for cloud transformation. Contributions include work as a contributor on the NIST 1800-3 ABAC (Attribute Based Access Control) standard and speaking events on identity access management and security.

# Data Superiority at the Tactical Edge

**Baron Rawlins, Lead Solutions Architect, AWS** • [awsbaron@amazon.com](mailto:awsbaron@amazon.com)

## ABSTRACT

Electromagnetic (EM) threats pose significant risk to operators at the tactical edge. AWS Data Analytics and AI/ML services can be used to counter these threats and provide EMS superiority to joint and Army CEMA forces at the point of need. The power of the cloud can be used in these settings to store, analyze and process historic electromagnetic reconnaissance (ER) and other data to train machine learning models to aid in the classification of EM emissions (target detection) detected in the EMOE and suggest or even direct the appropriate electromagnetic attack (EA) systems and countermeasures.

AWS data and analytics services in the AWS GovCloud and AWS Secret and Top-Secret regions can process available historic electromagnetic reconnaissance and other data. Using this data along with analyst input, AI/ML services can build high-fidelity classification models used to help detect hostile EM sources. Further, this data could be used to simulate the JEMSO actions that would be most applicable to deny or degrade the target. The models could be optimized via model quantization and other techniques and packaged in various modalities for edge deployment.

Through a cloud-to-edge pipeline, the models generated and packaged by the AWS AI/ML and analytics services can be deployed as discrete endpoint for inference on tactical edge hardware, such as the AWS Hybrid Edge family, specifically the AWS Snowball Edge and Snowblade, or the existing Tactical Server Infrastructure (TSI) hardware as fielded by PM-MC. Data from the available ES systems sensing the EMOE can then be sent to the models for inference to identify targets and suggest or direct action in support of the CEMA mission.

**BIO:** Baron Rawlins is a Lead Solution Architect in the AWS DoD Team. Baron has been instrumental in guiding Army Mission Owners to the cloud since joining AWS in 2020 after nearly 15 years at Cisco Systems supporting the DoD and Army on various programs. Baron's specializations include Networking, Security (DCO) and Machine Learning.

# Solving Bandwidth Limitations at the Tactical Edge by Using Dejero's Smart Blending Technology

**Bogdan Frusina, Founder, Dejero** • Bogdan.Frusina@dejero.com

## ABSTRACT

In the evolving landscape of modern warfare, the significance of resilient communication systems and effective management of information flow at the tactical edge is paramount. Dejero's Smart Blending Technology (SBT) addresses this challenge by ensuring all available network paths are maximally utilized simultaneously and seamlessly.

Dejero SBT is a new approach to connection (link) aggregation that delivers both improved reliability and faster aggregate connection speeds compared to other techniques. SBT achieves these outcomes by overcoming the technical challenges limiting most traditional connection aggregation solutions. In particular, Smart Blending uses granular, packet-based data distribution, enabled by real-time measurements of connection characteristics and enhanced by adaptive buffering and application acceleration. This design avoids the drawbacks of solutions that maintain flow stickiness and delivers superior performance with asymmetric connections like 4G LTE, 5G, and satellite (LEO/MEO/GEO) — making it especially valuable in mobile and nomadic situations.

As an alternative or enhancement to traditional connection aggregation (for example, in SD-WAN deployments), or as a viable option where other solutions are inadequate, SBT delivers significant advantages, including:

1. Achieving high link utilization and performance even with only a single flow, and even with unreliable connections.
2. Enabling particularly demanding applications, like low-latency constant bitrate video streaming.
3. Simplifying operational management and improving failover performance.
4. Administratively configuring connection priorities that dynamically and adaptively use the available links (in priority order) to achieve the target blended bitrates.

Moreover, SBT's containerized, software-based approach abstracts underlying connectivity, enabling end-to-end (including the access edge) orchestration of application-aware network services. All these elements combine to allow Dejero SBT to deliver reliable connectivity while still meeting demanding quality of service needs — in other words, to deliver reliable connectivity, anywhere.

**BIO:** As founder of Dejero, Bogdan Frusina is responsible for the strategic direction and vision of Dejero's innovative technology. Prior to creating Dejero's network aggregation platform, Bogdan began his career at Research In Motion (now BlackBerry) and has founded several start-up ventures.

# Hybrid Cloud in a Tactical World

**Brendan Kelly, Data Protection Specialist, Dell** • [brendan.kelly2@dell.com](mailto:brendan.kelly2@dell.com)

## ABSTRACT

Dell Technologies is the world leader in information technologies and boasts the world's largest IT — and data-related ecosystem. The U.S. Department of Defense is Dell Technologies' largest single customer, so it stands to reason that Dell has been focused on helping solve some of the DoD's most important data and IT problems. This solutions submission will broaden awareness of Dell's roles across tactical Hybrid Cloud Models; with a focus on data protection and cyber resiliency to ensure mission success. The emphasis will be on ensuring data at the tactical edge can be secured, protected and consumed, either on-prem or in the cloud. Dell intends to play a critical role in helping DoD organizations apply modern protection to an ever-evolving hybrid cloud world.

**BIO:** Brendan Kelly has been employed at Dell for the last 6 years and prior to that was at EMC. Over the past 4 years, Brendan has worked with customers across SOF, COCOMS, Army, USMC and the United Nations to drive mission-focused, results-oriented data protection and cyber resilient strategies.

# Enhancing Time-Based Analysis in Splunk Enterprise Security for Army Cyber Protection Teams

**Brent Matlock, Senior Consulting Solutions Engineer, Splunk •**

bmatlock@splunk.com

## ABSTRACT

Introducing a new feature in Splunk Enterprise Security (ES) that allows toggling between `_time` and `_indextime`, timestamps representing event and ingestion times respectively. This feature brings significant benefits to Army Cyber Protection Teams, enabling precise temporal analysis and investigation of security incidents. By switching between `_time` and `_indextime` during searches, teams can align their analysis with event chronology or ingestion order, gaining deeper insights, accurate timeline reconstruction, and the ability to uncover hidden patterns. This enhancement empowers Army Cyber Protection Teams to strengthen their incident response capabilities and fortify cyber defense strategies more effectively..



# Virtual Mobility at the Edge: Full Garrison Capabilities Using a Fraction of the Bandwidth

**Brian T. Kovalski, Senior Vice President, Federal, Hypori** • [brian.kovalski@hypori.com](mailto:brian.kovalski@hypori.com)

## ABSTRACT

The need for high bandwidth at the tactical edge is only increasing and as a result, so is the cost of purpose-built transmission systems to support this thirst for bandwidth. Hypori Halo is a virtual mobile device CSfC certified solution accessed from any smartphone, tablet, laptop or desktop running iOS, Android or Windows, that consumes less than 1Mb/s at its peak, while delivering the ability to view map data, threat feeds and use high bandwidth collaboration tools. Hypori Halo enables access to IL5 environments and full garrison capabilities at the tactical edge using a fraction of the bandwidth required.

**BIO:** Brian has 20+ years' experience as an information technology and intelligence professional and more than a decade of successful business management experience culminating as the CEO of Ski Systems. He began his career in the U.S. Army Signal Corps, where he served for 10 years. As part of L-3 STRATIS (now a CACI), Brian continued to support Military Intelligence and Special Forces activities after an honorable discharge. Brian has held positions from Senior Engineer, Program Manager to CEO, and has a track record of sustainable growth. Brian has a Bachelor of Science degree in information technology from the University of Phoenix.

# Virtual Mobility at the Edge: Gain Cross-Domain Access from a Single Device

**Brian T. Kovalski, Senior Vice President, Federal, Hypori** • [brian.kovalski@hypori.com](mailto:brian.kovalski@hypori.com)

## ABSTRACT

Hypori Halo is a CSfC-certified, virtual mobile device that enables access to on-prem and on-cloud environments up to IL5 from any smartphone, tablet, laptop or desktop running iOS, Android or Windows. Through our Hypori Private on-prem and on cloud approach, users can seamlessly transition from legacy on-prem services and cloud services as they move throughout the battlefield.

**BIO:** Brian has 20+ years' experience as an information technology and intelligence professional and more than a decade of successful business management experience culminating as the CEO of Ski Systems. He began his career in the U.S. Army Signal Corps, where he served for 10 years. As part of L-3 STRATIS (now a CACI), Brian continued to support Military Intelligence and Special Forces activities after an honorable discharge. Brian has held positions from Senior Engineer, Program Manager to CEO, and has a track record of sustainable growth. Brian has a Bachelor of Science degree in information technology from the University of Phoenix.

# The Future of Virtual Mobility at the Edge: Enabling Secure Comms with Command- and-Control Networks at Any Level

**Brian T. Kovalski, Senior Vice President, Federal, Hypori** • [brian.kovalski@hypori.com](mailto:brian.kovalski@hypori.com)

## ABSTRACT

Hypori Halo is a CSfC-certified, virtual mobile device that enables access to on-prem and on-cloud environments up to IL5. The Hypori Halo lightweight applications function on any smartphone, tablet, laptop or desktop running iOS, Android or Windows and its templates can be configured to support any voice and radio applications. At half the price of a smartphone, Hypori Halo is a cost-effective way to connect to Command-and-Control networks at any level.

**BIO:** Brian has 20+ years' experience as an information technology and intelligence professional and more than a decade of successful business management experience culminating as the CEO of Ski Systems. He began his career in the U.S. Army Signal Corps, where he served for 10 years. As part of L-3 STRATIS (now a CACI), Brian continued to support Military Intelligence and Special Forces activities after an honorable discharge. Brian has held positions from Senior Engineer, Program Manager to CEO, and has a track record of sustainable growth. Brian has a Bachelor of Science degree in information technology from the University of Phoenix.

# Enabling JADC2 Through Secure Data Security

**Chris Brown, Public Sector Chief Technology Officer, Immuta •**

chris.brown@immuta.com

## ABSTRACT

The Department of Defense (DoD) has recently published the Joint All-Domain Command and Control (JADC2) strategy that urgently calls for a focused push to empower U.S. joint force commanders with the capabilities needed to command the force across all warfighting domains and throughout the electromagnetic spectrum to deter, and, if necessary, defeat any adversary at any time and in any place around the globe. The strategy defines six lines of effort (LOE) including the establishment of the JADC2 Data Enterprise and to modernize Mission Partner Information Sharing. To successfully enable these two LOEs, the Army will need data security capability to operationalize data security policy at scale and work within the existing zero-trust mandates as well as the ongoing Army efforts to move to a data mesh architecture.

JADC2 recognizes the need for data-driven decisions to maintain battlefield superiority across land, air and sea. Yet, enabling warfighters and mission partners to quickly access data for decision making requires rethinking how data is managed, governed and secured so that only the right people can access the right data at the moment it's needed. Immuta offers solutions that address these topics:

- How Zero Trust and Data Mesh support the goals of JADC2.
- Why efficient data security will be necessary to implement the goals of JADC2.
- How the Army can automate the discovery, tagging and securing of data while integrating with existing enterprise tools such as Enterprise Data Services Catalog (EDSC).

**BIO:** Chris Brown is the Public Sector CTO of Immuta, whose mission is to enable the government to securely use data for the public good and protect the security of our nation. He is a leader, delivering cutting-edge digital solutions for customers across the DoD, the intelligence community, law enforcement and federal civilian agencies.

# Leveraging Cloud Computing to Overcome Bandwidth Limitations at the Tactical Edge

Chris Ernst, Senior Solutions Architect, AWS • chernst@amazon.com

## ABSTRACT

Bandwidth limitations at the tactical edge create significant challenges in efficiently pushing, receiving and analyzing information in real-time. Harnessing the power of cloud computing mitigates these limitations and enhances the capabilities of operations at the tactical edge. With cloud technology, data-intensive tasks can be offloaded to remote servers, reducing the burden on limited local resources and maximizing the potential for information processing and analysis. These benefits are realized through several cloud capabilities.

1. **Cloud-based Data Offloading:** Using cloud infrastructure, bandwidth-intensive operations such as data storage, processing and analysis can be moved from the tactical edge to remote servers. With this approach, tactical edge devices transmit only essential data for real-time decision making, optimizing bandwidth usage and reducing latency for critical operations.
2. **Edge-to-Cloud Communication:** A hybrid architecture that can use multiple modes of transport from commercial SATCOM and the internet to a cloud service provider's networking infrastructure can provide soldiers with flexibility and assists in overcoming bandwidth limitations where edge devices communicate strategically with the cloud. Rather than transmitting all data continuously, intelligent algorithms can selectively transfer relevant information, conserving bandwidth and reducing network congestion.
3. **Real-time Decision Support:** The cloud empowers tactical edge operations by providing access to extensive computing resources and analytics capabilities. Using machine learning, artificial intelligence and predictive algorithms in the cloud, real-time decision support can be offered to operators at the tactical edge that facilitates enhanced situational awareness, faster response times, and more informed decision-making.

**BIO:** Chris Ernst is a Solutions Architect on the AWS Army Team. Chris' focus is on cloud security, enabling zero-trust architectures from tactical edge to cloud. Prior to joining AWS, Chris spent 8 years with Cisco Systems supporting the U.S. Army with enabling software defined solutions.

# Hybrid Cloud Solutions

Chris Ernst, Senior Solutions Architect, AWS • [chernst@amazon.com](mailto:chernst@amazon.com)

## ABSTRACT

AWS supports the implementation of a hybrid cloud solution from cloud to tactical edge through our global infrastructure, infrastructure solutions and disconnected edge computing services.

Our Global Infrastructure starts with an AWS region, which is a physical location around the world where we cluster our datacenters. Each group of discrete data centers are referred to as Availability Zones (AZs), each with its own power, cooling, physical security and connectivity via redundant ultra-low latency networks. We support hosting workloads with various classification levels such as controlled unclassified information (CUI) in our isolated AWS GovCloud Region, accessed via a DoD Boundary Cloud Access Point (BCAP). For higher classification workloads, we offer air-gapped regions with the AWS Secret Region and Top-Secret Region, which are peered with SIPRNET and JWICS respectively. To enable classified connectivity from tactical edge to cloud, we offer soldiers multiple options to connect to AWS regions. These may include a dedicated network connection from on premises to AWS, providing routable access to our global network via our worldwide edge locations, reducing latency, improving availability and performance of your applications, and using AWS points of presence (POPs) worldwide via short haul connection to the AWS global network.

A core benefit of the AWS Global Infrastructure is that it enables secure access to our more than 200 fully featured services across our unclassified and classified regions, with service connectivity options that reduce operational burden on the soldier, regardless of their physical location. To move workloads and services closer to the soldier at a tactical operations center or regional hub location, AWS Infrastructure Solutions such as AWS Outposts can provide a hybrid cloud experience. Outposts extend a subset of a physical AWS regions services directly into an on-premises or edge location. For example, the AWS Elastic Compute Cloud (EC2) service enables workloads to be run locally, reducing latency and propagation delay while providing the same tools and APIs that soldiers are familiar with while running their workloads in the AWS Cloud. An additional AWS infrastructure solution such as AWS Private Local Zones can be used when mission requirements dictate, extending the AWS service footprint OCONUS while providing single-digit millisecond latency.

AWS disconnected edge computing services can be deployed to support workloads and services in dismantled and constrained tactical edge environments with limited or no network connectivity, allowing mission operations to continue in these environments. The AWS Snow Family — consisting of Snowball Edge compute and storage optimized devices, and Snowblade for a reduced SWAP envelope — allow for processing of data enabling real-time decisions and providing insights at the edge when cloud connectivity is not available. When connectivity is reestablished, data can be synchronized with applications running in the cloud for further processing using AWS analytics services to gain additional insights. The Snow family is capable of running several AWS services at the tactical edge to include compute, storage, networking, IoT, machine learning, security and third-party services, providing the soldier a full suite of tactical capabilities.

**BIO:** Chris Ernst is a Solutions Architect on the AWS Army Team. Chris' focus is on cloud security, enabling zero-trust architectures from tactical edge to cloud. Prior to joining AWS, Chris spent 8 years with Cisco Systems supporting the U.S. Army with enabling software defined solutions.

# Meeting the Need to Rapidly and Reliably Collect and Convert Messy Data and Signals into Actionable Intelligence

**Christopher Stephenson, Head of AI Operations, Nuix** • [chris.stephenson@nuix.com](mailto:chris.stephenson@nuix.com)

## ABSTRACT

Like all organizations (large or small, government or corporate) collecting, processing and interpreting digital data is becoming increasingly challenging. These challenges are exacerbated by tightening budgets, aging technologies, rapidly shifting needs and constant increases in the volume, variety and velocity of data that must be mastered to ensure successful missions. As a crucial division of the Army, the Cyber Center of Excellence (CCOE) carries the additional burdens of helping to ensure national security, military readiness and global stability. All this raises the stakes on rapidly and reliably collecting and converting messy data and signals into actionable intelligence for timely, life-saving decisions.

Nuix technology is currently in use across the U.S. government (including the DOJ, DoD, FAA and more) and around the world, supporting massive and complex investigations, including Panama Papers, Diesel-Gate, and Grenfell Towers. If it hits the front page of the newspaper, chances are Nuix software was used behind the scenes.

To solve the CCOE's challenge of quickly and accurately correlating omni-channel data to inform the commander of emerging risks, Nuix offers a commercial-off-the-shelf (COTS) software platform called 'Neo.' Based on more than two decades of global leadership in data intelligence — and featuring a patented data processing engine and MIT-award-winning AI at its core — Neo is uniquely positioned to offer a seamless and integrated platform that can automatically classify, contextualize, correlate and prioritize Army data to optimize intelligence gathering and decision-making.

Nuix Neo consumes data from structured, semi-structured and unstructured sources (covering 1000+ file/data types, including: communications, webpages, office documents, text, PDFs, AWS S3, Office 365 and more), extracts the text and metadata into a normalized schema and provides a variety of user interfaces optimized to provide actionable information to multiple different organizational roles. The information is normalized into a unified repository, and made available for search, analysis, reporting and export. All of this happens “out of the box,” with zero custom development or coding.

In addition to extracting the raw content, Nuix provides various levels of analytic enrichment to improve usability, efficiency and usefulness. This includes features like optical character recognition and auto classification of image/photos; condensing entire videos into a thumbnail view to enable rapid screening of content; and shingling content to find similar text across vast quantities of data.

Nuix also offers Natural Language Processing (NLP), a cutting-edge deep learning capability that delivers highly accurate document classification, content categorization and enhanced entity extraction across all the normalized content. Nuix NLP goes beyond just AI/ML and delivers organizational outcomes with its built in Risk Engine. The Nuix NLP Risk Engine builds aggregate scores for each piece of content using multiple facets of an item's content to help narrow the focus onto the data that matters most.

To further extend the value for CCOE's data correlation use case, Nuix Neo offers graph-based link analysis that provides dynamic, interactive visualizations and alerting, to reveal previously unknown relationships across your data.

Lastly, working in tandem with Neo is Nuix Adaptive Security (NAS), which is an end-point product that provides the market's most comprehensive set of User Activity Monitoring (UAM) features. NAS can be used as additional data collection capability and another "set of eyes" at the desktop level, create a 360-degree view of US-AR data.

The submission outlines how organizations like the Army quickly and flexibly make sense of data from a vast array of sources and file types using Nuix Neo's highly differentiated features and capabilities including:

- No-code natural language processing, which empowers non-technical staff to build, validate and optimize text analysis models quickly and easily without a single line of code.
- Integrated, end-to-end data processing platform (from collection to granular, actionable data) with a single sign-on.
- Thousands of out of the box text analysis models to optimize time to value.
- Flexible deployment options include on prem, cloud-based or hybrid options.
- 1000+ file types supported for ingestion and indexing.
- Graph-based link analysis of structured and unstructured datasets.
- Optional end-point user monitoring, including automated screen capture and forensic exfiltration, in addition to identifying and containing insider threats.



**BIO:** Chris Stephenson is a highly accomplished professional with a diverse background in operations, business development and co-founding successful technology companies. With a strong focus on artificial intelligence and natural language processing, Chris has consistently delivered outstanding results throughout his career.

Currently serving as the Head of Operations, NLP at Nuix, Chris spearheads the development and implementation of cutting-edge NLP solutions. Leveraging his expertise in AI, he enables organizations to harness the power of next-generation NLP technologies, allowing them to build advanced text analytics models quickly and efficiently.

Chris also holds the position of Director & Vice President at the Peter H. & Dana Gunn Winslow Foundation, Inc., where he actively contributes to fostering a more equitable society through early educational opportunities for underprivileged pre-school children in Washington, D.C.

As the CEO/Co-founder of Topos Labs (now Nuix NLP), Chris played a pivotal role in revolutionizing the field of NLP with their groundbreaking No-Code AI software, “Gracie.” This cognitive computing platform empowers non-technical teams to create sophisticated text analytics models without the need for coding. Gracie’s accuracy surpasses traditional machine learning approaches, making it a game-changer for industries such as financial services, government/DoD, and cybersecurity.

Chris’s contributions to the field of technology extend beyond software development. Holding a patent for the Digital Content Enhancement Platform, he and his team pioneered a revolutionary method for end-users to seamlessly search multiple supplemental internet data sources, including Wikipedia, YouTube, Flickr and more. This innovative platform allows users to interact with keywords from originating content without opening new browser tabs or windows, eliminating the need to leave the original page.

In addition to his professional achievements, Chris has been actively involved in various organizations, including the National Small Business Association, Small Business Technology Council, and BUILD. Through his mentorship and guidance, he has played a vital role in using entrepreneurship to inspire and guide low-income students towards academic success.

# Focusing on Data Without Ignoring Voice Communications

**Courtney Stiles, Director of Business Development, REDCOM Laboratories, Inc. •**

courtney.stiles@redcom.com

## ABSTRACT

According to the U.S. Army Cloud Plan, the current goal for the United States Army is to reduce its 12 remaining data centers to five by 2028 and converge hundreds of installation processing nodes worldwide. To achieve this goal, the Army must strike a balance between taking advantage of the power of the cloud, when it is available, and a way to conduct operations, when it is not. When the U.S. Army talks about implementing off-premise hyperscale, on-premise, and hybrid cloud, the focus is always on data. Where to store the data, how to filter the data and how to get the right data to the point of need, at the right time. While these are important and challenging tasks, voice communications is still an important factor in Command and Control and cannot be ignored. REDCOM focuses on incorporating voice, in addition to data, into the hybrid cloud environment to provide federated voice, chat, video, conferencing and radio interoperability characterized by attribute-based access on the classified and unclassified side. Benefits of using a REDCOM solution include:

- Hardware, hypervisor and cloud deployment
- Security: Built-in security pre-requisites
- Operational Flexibility & Resiliency: Secure Clients support registering to multiple accounts simultaneously. Local software instances provide local survivability when the cloud is not available
- Reduce maintenance, lifecycle, and training costs: REDCOM solutions in use within the U.S. Army today in tactical environments

**BIO:** Courtney Stiles is Director of Business Development for REDCOM Laboratories, Inc.

# Operationally Effective and Non-Cost Prohibitive Technology to Provide Secure Communications Components of Converged C5ISR/EW Systems

**Courtney Stiles, Director of Business Development, REDCOM Laboratories, Inc. •**  
courtney.stiles@redcom.com

## ABSTRACT

In secure voice communications, multiple hardware and software solutions are often cobbled together to provide mission-critical capabilities. On top of that, many of these solutions only work in proprietary eco-systems. The result is a complex, increasingly hard-to-manage solution set as each of these individual products need to be procured, configured, tested and documented. Subsequent upgrades require additional testing, which compounds the effort required to maintain a multi-vendor solution. Advancements in technology often increase complexity and add to the cognitive burden of the warfighter. Furthermore, these multi-vendor solutions require extensive training and re-training of personnel and contractors in theatre, impacting operational readiness. This is notably expensive and time-consuming, especially with the personnel changes that occur regularly. The most operationally effective and non-cost prohibitive technology to provide secure communications components of converged C5ISR/EW systems to pass verbal information that enables tactical unit leaders as part of the division as a unit of action in Army 2040 must be:

- Interoperable with existing equipment while enabling the rapid insertion of new technologies
- Operationally flexible: able to communicate over any available spectrum or network with capabilities that seamlessly transition between those resources
- Intuitive and easy-to-use
- Scalable to support any force structure responding to any crisis across the full range of military operations
- Expeditionary: quickly establish communications and integrate with assets during a variety of missions, using a variety of capabilities, and force assortments

**BIO:** Courtney Stiles is the Director of Business Development for REDCOM Laboratories, Inc.

# Enabling Hybrid Cloud With Cloud Ready Networks

**Craig Hill, Distinguished Architect, U.S. Public Sector – CTO, Cisco •**

crhill@cisco.com

## ABSTRACT

As the Army evolves toward hybrid cloud and considers the implications of applications transitioning from the on-premises data centers to remote, less controlled commercial public clouds, Infrastructure as a Service and/or Software as a Service (IaaS/SaaS), one of the critical factors is application “location.” Application “location” is having an impact on several indirect factors, such as how agencies approach next-generation wide area network (WAN) design requirements, but also security. Controlling the access to applications that reside in locations with far less visibility and control (in the public cloud) than in their localized on-premises data centers becomes much more important.

Addressing this problem is where the concept of a new architecture called the Cloud Ready Network (CRN) comes in. CRN provides a new framework for IT organizations and architects to define a “cloud edge” demarcation. This architecture targets a secure and intelligent WAN domain, typically through a Software Defined WAN (SD-WAN) fabric. And it defines a new “meet me” point or “cloud edge” — most efficiently using co-location centers — to establish that security control point for any traffic leaving the agency.

Diving deeper into the benefits of a well-equipped SD-WAN, the solution enables a “Data-Centric” environment and at its core, a foundational network constructed with the ability to support mass-of-maneuver forces in various/multiple theaters of operation. The Army must leverage a highly flexible infrastructure to support the ever-changing requirements at the tactical edge.

Benefits to the tactical edge are as follows:

- **Greater agility:** Traditionally the Army has required net new infrastructure to support any emerging crisis. This inefficiency due to security slows the pace of operations, increases complexity, and limits communication and collaboration among necessary partners. The Army can leverage segmentation to architect a solid fixed core SD-WAN environment spanning the Enterprise, Regional Locations, Tactical Forward Operating Locations and tactical nodes that are able to flex rapidly for specific mission needs without severe network impacting changes and undefined infrastructure costs.
- **Simplified Traffic Management:** SD-WAN policy definitions within a single fabric allow for traffic to be constrained within a defined geographic location. With proper site-ID management on a per geographic region, traffic is allowed within the defined regions locations, thereby allowing the Army to rigorously control traffic flow and adapt it to rapidly changing mission circumstances.
- **Better user experience:** Provides a consistent user experience, regardless of where the application resides, with application-aware routing that leverages intelligent forwarding based on latency, loss, and jitter.

- **Integration of multiple transports:** The management and integration of independent multi-domain transport links such as MPLS, satellite, microwave or broadband becomes seamless and obscure via a centralized management platform.
- **Threat-centric security:** Securely connects your users, devices and applications with Cisco's embedded security stack (firewall, IPS, URL-filtering, malware protection and cloud protection).
- **Extensive cloud integrations:** Enhances multi-cloud application experience with technology partnerships from AWS, Google Cloud, Microsoft, Equinix and Megaport across any location.
- **Proven scalability:** The sheer size of the Army demands a capability that's able to deliver a cloud-scale SD-WAN solution with proven large deployments of up to 10,000+ sites.
- **Actionable insights:** Provides end-to-end visibility into application, internet and cloud environments, enabling agencies to identify and troubleshoot issues more quickly.

Cisco SD-WAN bridges intelligent, application aware networking and security to deliver a flexible architecture that is built upon a zero-trust model. Cisco SD-WAN seamlessly connects devices and people to any cloud, providing a superior application experience while delivering consistent unified threat protection from branch to cloud.

**BIO:** Craig Hill is a Distinguished Architect in the U.S. Public Sector CTO office having been at Cisco for 28 years, focusing on large end-to-end architectures in the DoD, U.S. intelligence and global enterprise networks. Recent focus is on designing global WAN service architectures with IP/MPLS and Segment Routing, SD-WAN/SASE/zero trust and customer network transitions to the public cloud. Other focus areas include high-speed encryption, recent Quantum safe solutions, network and cloud visibility using ThousandEyes and other tooling and transitions to automation/orchestration DevOps environments. Craig is a 28-year CCIE in Routing and Switching and is based out of the Northern Virginia/Washington D.C. area.

# Leveraging Neuromorphic Technology in Today's Battleground and Turning Raw Data into Actionable Information for Commanders at the Edge!

**Jason K. Dunn-Potter, Solutions Architect & Mission Specialist, Intel** •

[jason.dunn-potter@intel.com](mailto:jason.dunn-potter@intel.com)

## ABSTRACT

How do we survive and thrive in an ever-evolving digital battlefield? Short answer: We adapt! Incorporating new technology has proven the key to decisively winning and those who have failed to quickly and effectively adapt new technology have done so at their peril. History is littered with examples — tanks in (WWI), aircraft carriers (WWII), GPS (Desert Storm) all have provided decisive advantages. Tomorrow's leap in technology is all going to revolve around cyber battlefields. Specifically, who can sense threats to their digital systems and mitigate them quickly. The adage “knowledge is power” has never been more prevalent than today's digital landscape. To address this, Intel Corporation and the defense industry has been making enormous strides in providing technologies to identify threats and provide countermeasures.

One way to address this is a new technology that Intel has worked with Lewis Rhodes Labs (LRL) to create called Neuromorphic Processing Units or NPUs. NPUs are a completely new capability. The “NPUs” are changing how we collect, organize and access data. Based on neurology, NPUs change how data can be queried and used. Placing an NPU on top of your data storage can make all the difference. Gathering data through sensors, log generators and other inputs has never been the real problem. Sifting, sorting, organizing and extracting that data has plagued organizations since the beginning of data. NPUs address that problem and significantly reduces the impact by allowing unorganized, unindexed (i.e., raw) data to be swiftly searched and extracted. Combing more than 80 gigabits per sec per server!

The key takeaway is today's data centers can collect data in whatever format and store in any file structure they want. NPUs can query it all in near real time and in seconds it can provide your systems with the critical data you need to identify, extrapolate and action. Additionally, NPUs can work in tandem at multiple locations to provide distributed query capability and provide a unique capacity that delivers results. This feature is decisive as bandwidth will continue to be the limiting factor. NPUs can augment your existing architectures and does not require expansive recoding or removing any existing architectures. It is a physical component that optimizes your operations and has been implemented by the U.S. government today!

Key takeaways:

1. Actioning critical information is the cornerstone of success in a digital battlefield.
2. Neuromorphic technology is being deployed today across the federal government.
3. Leveraging NPUs will revolutionize how you conduct data operations.
4. Enhancing search capabilities will directly improve C2/COP, ISR, OCO and DCO operations.

**BIO:** Jason K. Dunn-Potter currently serves as a Solutions Architect & Mission Specialist supporting the U.S. Department of Defense under our Public Sector team for Intel. Joining the team in 2021, Jason has been responsible for technical solutions supporting all public sector including federal, state, Department of Defense and national security organizations. Additionally, he is the principal technical support to DoD elements and covers all facets defense.

Prior to joining Intel, Jason served as an U.S. soldier for more than 26 years, where he achieved the rank of chief warrant officer 5 (CW5) and held numerous leadership & technical positions. In his previous role he served as the Command Chief Warrant Officer (CCWO) aka Chief Technology Officer (CTO) for the White House Communications Agency (WHCA), where he focused on long-term strategy, talent management and innovative changes. As part of the command suite, he helped lead more than 1,400 joint servicemembers comprising active, National Guard and Reserve personnel for all the military branches. Across the Army, he has worked in various technology roles, including cybersecurity, systems management, networking and policy. He started his career as a 31U (now 25U) and worked as a radioman & systems repairer. He served in five infantry divisions, spending most of his time in armor, artillery, combat engineers and other tactical units. He also spent years in various NETCOM commands and served as the HRC Assignment Officer managing more than 1,300 signal warrant officers matching talent to tasks across the entire Army and joint organizations.

Jason is a published author and leader on information technology topics, including digital efficiency, cybersecurity, transmission technologies and optimization strategies. He is actively involved in educating the U.S. government and regional emerging leader programs. He is an aggressive civil leader and is a lifetime member of several organizations that promote DoD spirit-de-corps and technology enhancement. He also holds a master's degree in IT management from Grantham University and has held a current CISSP for more than a decade, along with various industry technical certifications from Microsoft, Cisco and others.

# How Intel is Building Hybrid Clouds to Maximize Operations

**Jason K. Dunn-Potter, Solutions Architect & Mission Specialist, Intel •**

jason.dunn-potter@intel.com

## ABSTRACT

Intel is a world leader in building clouds and has dedicated teams supporting each of the major cloud service providers (CSP) enhancing all cloud architectures hardware and software. We have an army of dedicated cloud support architectures aligned to each of the CSPs. Today, Intel is continuing to build and enhance cloud capabilities. Leveraging a hybrid solution brings significant value especially in a DDIL environment.

Cloud is more than just another server hosted by a third party — much more. True cloud environments operate off fundamental principles that define not just cloud architectures but productivity enhancements. Intel has proven in every industry that cloud can boost operations, bring critical tools to the edge and remove physical barriers that often arise from LSCO and HA/DR operations. Operational environments require agile abilities, physically and digitally. Tomorrow's missions will be decided not by who has the largest force, but by how to achieve optimal results through information and decisive action. Enabling all echelons of command to maintain situational awareness and maneuverability will be a key decisive advantage. Cloud operations can enable that through many ways including:

1. **Data redundancy** — Ensuring data you need is protected and available from sensor to shooter to sustainer and beyond.
2. **Data Accuracy through Analytics** — Leveraging tools like AI, GPUs and predictive analytics will provide the real-time information commanders need to make key decisions.
3. **Data Displacement** — Hybrid cloud environments allow commanders at the edge in a DDIL environment to fight while engaged, but at the same time allow each supporting echelon to bring the full capabilities of the DoD. This is accomplished by sharing real-time information across all echelons, limiting wasted time and talent making reports.
4. **Data Integrity** — Enhancing the security posture as data moves from the edge to HQ. This is continuing to challenge organizations and is why we are exploring confidential computing capabilities for all cloud providers. Keep the admins out of your data.



Some of the tools include:

- A. **Confidential Computing** — Building data isolation and controls inside of a shared cloud environment is the future of cloud. Intel is partnering with the entire ecosystem to integrate this capability.
- B. **Granulate (tools)** — Optimization of cloud workloads can significantly enhance results. There is a litany of tools that are available to enhance operations.
- C. **Planning** — As with all missions, you need the right knowledge to make smart decisions about how to get the most out of the environment.

Today Intel works with the DoD to aid in leveraging the full capability that a cloud can provide while ensuring commanders on the edge retain the needed capabilities to survive in a DDIL environment.

**BIO:** Jason K. Dunn-Potter currently serves as a Solutions Architect & Mission Specialist supporting the U.S. Department of Defense under our Public Sector team for Intel. Joining the team in 2021, Jason has been responsible for technical solutions supporting all public sector including federal, state, Department of Defense and national security organizations. Additionally, he is the principal technical support to DoD elements and covers all facets defense.

Prior to joining Intel, Jason served as an U.S. soldier for more than 26 years, where he achieved the rank of chief warrant officer 5 (CW5) and held numerous leadership & technical positions. In his previous role he served as the Command Chief Warrant Officer (CCWO) aka Chief Technology Officer (CTO) for the White House Communications Agency (WHCA), where he focused on long-term strategy, talent management and innovative changes. As part of the command suite, he helped lead more than 1,400 joint servicemembers comprising active, National Guard and Reserve personnel for all the military branches. Across the Army, he has worked in various technology roles, including cybersecurity, systems management, networking and policy. He started his career as a 31U (now 25U) and worked as a radioman & systems repairer. He served in five infantry divisions, spending most of his time in armor, artillery, combat engineers and other tactical units. He also spent years in various NETCOM commands and served as the HRC Assignment Officer managing more than 1,300 signal warrant officers matching talent to tasks across the entire Army and joint organizations.

Jason is a published author and leader on information technology topics, including digital efficiency, cybersecurity, transmission technologies and optimization strategies. He is actively involved in educating the U.S. government and regional emerging leader programs. He is an aggressive civil leader and is a lifetime member of several organizations that promote DoD spirit-de-corps and technology enhancement. He also holds a master's degree in IT management from Grantham University and has held a current CISSP for more than a decade, along with various industry technical certifications from Microsoft, Cisco and others.

# Data Approaches to Improve Mission Effectiveness

**Dr. Paul Lieber, Chief Data Scientist, Peraton** • paul.lieber@peraton.com

## ABSTRACT

The quest for the perfect common operating picture (COP) is one many commanders long for — only to be sorely disappointed. Much of this disappointment and falling short stems from disconnected systems and knowledge management issues that separate data sources and analysis workflows. Thus, and sadly until present, most deeper analyses required to properly gauge risk and opportunity to ongoing missions remains a laborious and manual one executed by a large set of analysts siloed by classification level.

Even with the introduction of AI and ML capability to automate data analysis processes and identify meaningful relationships, application of this capability remains rudimentary. Current paradigms favor additional tool adoption versus true capability integration, which only exacerbates the challenge by spending dollars but rarely moving the know-how needle. Specifically, more insights do not necessarily produce enhanced understanding of any mission risk or opportunity.

Moreover, data platforms are useful in accessing multiple tools and solutions across hybrid cloud environments, but these too feature isolated API or data feeds as part of any common operating picture creation. Once more, and in this stage, this picture requires heavy analyst effort to ascertain how the sum of the COP parts warrants additional looks plus — if available — more data feeds (often at higher classification levels) to create informed recommendations of value.

Recommending an alternative and one currently conducted by Peraton: commanders and their staff are missing a golden opportunity to pivot these platforms and centralized AI and ML models to identify purposeful data relationships (i.e. configuration, associations, time series, etc.) across various tools and streams. In tandem, to apply a series of even simplistic data structuring to allow co-mingled analyses and visualizations to occur. Also, and importantly, apply automation — assisted by human SMEs — to highlight normalized data presentations across a data lake and to auto-construct threat and opportunity scores which can account for normalized event data distribution and standardized deviations.

These steps also allow for ML predictive modeling to proactively identify risk and opportunities to mission informed by anomalies that occur — and with confidence. Inserting and semi-structuring supporting data feeds only enhances confidence in findings, while — once more — better pivoting human analysts toward directions of greatest need. It's about training the models and analysts, simultaneously, to work together.

Still, to get to the alternative would be a dramatic contrast that requires a re-think of technology adoption cycles and execution with a now greater premium on data integrators, risk/opportunity data model development and maintenance, also workflows and UI/UX to ensure rich data analyses are providing insights in a familiar and actionable fashion for end users. For example, the structure and process build of joint visualization is vital in storytelling, even with high confidence risk and opportunity information indicating a need for attention.

Also, all this counters an argument for more data sources and tools by default, rather to emphasize integration and re-purposing first and foremost. Historical data must be considered as part of risk or opportunity assessments to standardize data models, likewise, to create time series enactments of what future battlespace conditions may look like under adjusted parameters.

**BIO:** Dr. Paul Lieber is Peraton's Chief Data Scientist for its Cyber Mission Sector, where he provides executive strategic guidance on sector approaches and investments to data usage and application. He likewise serves as an Associate Research Scientist at the University of Maryland's Applied Research Laboratory for Intelligence and Security, offering expertise in data science-driven modeling and assessment of influence toward vulnerable populations within social media environments. Formerly COLSA's Chief Scientist, Paul functioned as the command writer for two USSOCOM commanders and strategic communication adviser to the commander of Special Operations Command-Australia.

Within academic environs, Paul was a full-time member of the Graduate faculty at Joint Special Operations University, Emerson College, University of South Carolina, and the University of Canberra, respectively. Within these roles, he taught across the entire strategic communication and influence curriculum, with a research emphasis on social media-based persuasion and methodological design. He possesses nearly 100 combined publications and lectures on these topics.

# Hybrid Cloud Solutions — A Bridged Approach

**Dr. Paul Lieber, Chief Data Scientist, Peraton** • paul.lieber@peraton.com

## ABSTRACT

As evidence and for a select DoD customer, Peraton teamed with a leading technology company and cloud solutions provider to provide a centralized data platform and visualization capability within an IL5 cloud environment; and employed this company's proprietary API integration and native AI/ML models (8000+) to establish a singular point of program entry featuring custom dashboards by user type. Importantly — and as Peraton and this customer possess key relationships with an array of cloud services providers — this solution was deliberately designed to fuse with said customer's sister cloud environments and all relevant resources (data and tools) within.

To further embrace environment agnosticism and reduce capability abandonment (via disconnected offerings), this Peraton hybrid cloud solution was likewise buoyed by an array of complimentary Peraton IR&D/Labs offerings also select partner data feeds and supporting tools. Combined, this yielded advanced methods for conducting AI-driven network analysis and pattern assessment, semi-structuring of data to locate relationships, data entropy and pattern of life modeling, among others.

For this customer, additional careful consideration was given to ensure compatibility with existing workflows and doctrine native to them. Thus, and across the Peraton hybrid cloud solution, assessment steps and visualizations are executed, captured and reported in alignment with customer doctrine and practice norms. Finally — and as important for this customer — select assessments from the Peraton hybrid cloud environment are semi-structured and transported via a validated data gateway to a secondary IL6 hybrid cloud environment for subsequent assessment and consideration of additional and potentially classified, relevant data feeds.

Being future leaning, supporting Peraton lab and partners continuously build, refine and test AI and ML models to ensure hybrid cloud integrity also a more proactive response to emerging problems requiring new models or otherwise. Specifically, this support serves as needed assurance no updates/improvements to any part of the Peraton hybrid cloud solution renders it incompatible.

Holistically and in contrast to other approaches to hybrid cloud solutioning, Peraton sought to deliberately bridge not just host relevant environments and tools alongside others. This included establishing a central platform, sign on, and data lake to create program and process efficiencies, also a mechanism to conduct cross-platform assessment. Supporting continuous process improvements and an emphasis on reducing integration cost ensures reduced burdens from changing technology and emerging requirements. Last, alignment with customer workflows and doctrine maximizes buy-in and return on investment.

**BIO:** Dr. Paul Lieber is Peraton's Chief Data Scientist for its Cyber Mission Sector, where he provides executive strategic guidance on sector approaches and investments to data usage and application. He likewise serves as an Associate Research Scientist at the University of Maryland's Applied Research Laboratory for Intelligence and Security, offering expertise in data science-driven modeling and assessment of influence toward vulnerable populations within social media environments. Formerly COLSA's Chief Scientist, Paul functioned as the command writer for two USSOCOM commanders and strategic communication adviser to the commander of Special Operations Command-Australia.

Within academic environs, Paul was a full-time member of the Graduate faculty at Joint Special Operations University, Emerson College, University of South Carolina, and the University of Canberra, respectively. Within these roles, he taught across the entire strategic communication and influence curriculum, with a research emphasis on social media-based persuasion and methodological design. He possesses nearly 100 combined publications and lectures on these topics.

# Data Protection at the Edge

**Gina Scinta, Deputy Chief Technology Officer, Thales TCT •**

Mary.Shiflett@ThalesTCT.com

## ABSTRACT

Core computing functionality commonly found in data centers and in the cloud is also being deployed at the edge — data protection capabilities must transition with that move. However, many challenges often stand in the way of extending core-level security to the edge. Harsh environments; bandwidth-limited and disconnected sites; overrun or hostile scenarios; and constraints related to size, weight, and power have made it difficult to employ the appropriate levels of security while allowing the kind of quick response needed at the edge.

True data protection extends to edge. Thales TCT presents how to apply the same level of security deployed in the core and the cloud to edge environments and offers:

- How to contend with environmental and operational constraints at the edge
- How to extend your existing cybersecurity infrastructure to the edge
- Why supply chain security is critical at the edge

**BIO:** Gina Scinta is Thales TCT's Deputy Chief Technology Officer (CTO). In this role, Gina serves as the company's technology evangelist. Her mission is to help Thales TCT's U.S. federal government customers learn effective ways to solve their mission critical cybersecurity challenges. Gina also leads several strategic initiatives for the company, such as the collaboration with NIST National Cybersecurity Center of Excellence, ACT-IAC and more.

Gina has more than 30 years of experience in the technology community. Prior to joining Thales TCT, Gina served as a senior solutions architect with Thales Digital Identity & Security. In this role, she focused on providing solutions for protecting data using world-class encryption and key management for data at rest in data centers and cloud infrastructures.

# Protecting Your Data in Their Cloud

**Gina Scinta, Deputy Chief Technology Officer, Thales TCT •**

Mary.Shiflett@ThalesTCT.com

## ABSTRACT

Cloud Service Providers (CSPs) emphasize the shared responsibility model for securing data in the cloud and meeting compliance requirements for information protection. CSPs own the responsibility to secure the infrastructure that runs their cloud services. Data owners are responsible for protecting the confidentiality, integrity and availability of their data in the cloud.

Making sure that this data is safe from unauthorized access requires organizations to consider not only the physical and logical security of the CSP but also who is encrypting the data; when and where the data is being encrypted; and who is creating, managing, and accessing the encryption keys.

Thales TCT presents how to reduce the risks associated with storing sensitive data in the cloud and addresses these topics:

- Meeting compliance and regulatory mandates
- Applying customer-owned encryption and key management
- Deploying a hybrid cloud for increased security
- Utilizing multiple cloud providers effectively

**BIO:** Gina Scinta is Thales TCT's Deputy Chief Technology Officer (CTO). In this role, Gina serves as the company's technology evangelist. Her mission is to help Thales TCT's U.S. federal government customers learn effective ways to solve their mission critical cybersecurity challenges. Gina also leads several strategic initiatives for the company, such as the collaboration with NIST National Cybersecurity Center of Excellence, ACT-IAC and more.

Gina has more than 30 years of experience in the technology community. Prior to joining Thales TCT, Gina served as a senior solutions architect with Thales Digital Identity & Security. In this role, she focused on providing solutions for protecting data using world-class encryption and key management for data at rest in data centers and cloud infrastructures.

# Hybrid Cloud Adoption on the Forward Edge of Battle

Hansang Bae, Public Sector Chief Technology Officer, Zscaler • hbae@zscaler.com

## ABSTRACT

The Forward Edge of Battle Area (FEBA) is more dynamic than ever. And battle plans need to adjust in the modern battlefield, where it is no longer just about beans and bullets but beans, bullets and BITS. Information is as important as “combat load” to be successful. To adapt to the dynamic FEBA, commanders will need more information to defeat the enemy. In addition, the soldiers on the ground will require up-to-the-minute information to react to the changing FEBA but also to deliver the right set of information to the commanders. This agile access cannot be provided using legacy equipment with a long tail of organic support requirements. By adopting hybrid clouds that can be projected to the frontlines, zero-trust principles can be adhered to even on the battlefield. Zscaler, together with Klas Government, gives commanders proven technologies that can make this adoption seamless, enabling dynamic need to know access, to data in the cloud or on the tactical edge.

**BIO:** Hansang Bae has more than 25 years of experience working in the information technology industry. As Zscaler’s Public Sector CTO, he is responsible for assisting and educating customers in their digital transformation journey. He is not only well versed but also passionate about his role in advising public sector organizations on best practices and strategies for adopting a cloud-first security posture.

During his career, Hansang has served in similar roles as an executive member at Netskope and at Riverbed. Prior to Riverbed, he was a member of the Citi (Citigroup) Architecture and Technology Engineering leadership team. As one of the six global engineering leads, he was responsible for data center, branch and performance engineering, network management (NMS) tools, and capacity planning groups for all of Citi.

As an avid protocol analyst, Hansang collaborates with industry associations in educating public sector organizations and also holds an active role as a board member of Wireshark Foundation, helping steer the open-source project and ensure its continued success.



# Digital Twins, Driven by a Secure COTS Cross Departmental Data Mesh, Advance Decision Making to the Speed of Relevance

**Jacques Jarman, CRO, Edge Technologies** • [jacques.jarman@edgeti.com](mailto:jacques.jarman@edgeti.com)

## ABSTRACT

The Department of Defense maintains millions of mission-critical data sets, many duplicative in nature, siloed within agencies and departments. Today's threats are forming and exercised, at a speed never seen. Commanders need access to the right information at the speed of relevance. Unfortunately, the information stored in these multiple systems is hard to access, and in some cases, unknown to the decision maker.

To solve this issue, data must be democratized, discoverable and made securely available to the people who need it at the moment it is needed. Past attempts at large data warehouses and data lakes have resulted in incomplete solutions and over budget projects. Moving forward, the Defense Department needs to develop a comprehensive data mesh that will allow decision makers to access the data in its authoritative system.

With a comprehensive data mesh in place, decision makers will be able to construct mission-specific digital twins of their mission environment, crossing departmental and application boundaries, to get a complete common operating picture (COP) of the mission at hand. With the data mesh in place, these COPs can typically be constructed and operational in days.

Edge Technologies discusses the practical application of the first commercially proven data mesh platform, edgeCore, including past performance examples within DoD and some of the largest global enterprises.

Recognized as an innovator in the digital twins marketplace by Gartner and an ABMS contract holder in support of the Air Force's contribution to JADC2, Edge Technologies' (Edge) Data Mesh platform, edgeCore, has been ATOed on NIPRNet, SIPRNet, JWICS and DREN, and used in all branches of DoD over the past two decades.

edgeCore's transformational approach to data integration and visualization integrates data within existing ATOed solutions in real time, securely in agency datacenters or cloud environments, without creating a new persistent data store. The result — a mission-optimized data mesh that offers Data-as-a-Product to address the unique requirements of the mission.

edgeCore achieves this by utilizing a Built for Purpose platform that includes the following features:

- Role-based access control, fully authenticated Single Sign-On (SSO) access
- LDAP, AD, Kerberos, NTLM, 2FA, CAC, and more identity providers supported
- Highly secure and scalable multi-tenant architecture (enable/enforce)
- Flexible deployment configuration options for data protection across enclaves
- Web-layer integrations for existing application UIs
- Data-layer integrations, transforms, filters, merges, correlations and visualizations
- Ability to trigger runbooks, workflows, RPA and orchestrate third-party systems
- HTML5-based with adaptive layout and mobile device support

Today's existential challenge is getting the right information to the right people at the right time at the speed of relevance. There is no shortage of data, there is often too much data, in the form of redundant copies stored in numerous data warehouses and data lakes. Traditional solutions require combining data in new data repositories to break down data silos and provide mission critical insights. Unfortunately, that method rarely results in a comprehensive solution and almost always takes much longer to implement than originally estimated. A secure data mesh is a better, faster, more secure and more cost-effective alternative.

•

**BIO:** Jacques Jarman is the CRO at Edge Technologies. Jacques is focused on setting corporate direction to meet the needs of edge's customer base. With more than 25 years of experience working with the DoD and civilian agencies, Jacques oversees federal operations. He is an invited speaker and holds a Bachelor of Science from Virginia Tech.

# The Ultimate Flexibility in Hybrid Data Management and Data Analytics

**James S. Herron, Solution Engineer, Cloudera Government Solutions, Inc. •**

[jherron@cloudera.com](mailto:jherron@cloudera.com)

## ABSTRACT

As the Army's vision and strategy for cloud modernization continues to evolve, it must encompass an enterprise-class data management platform supportive of a hybrid-cloud deployment framework to enable the warfighter to gather, structure, analyze, discover, consume and share data.

Cloudera, a leading enterprise data management solutions provider, offers a range of products to help the Army accelerate its strategic intent. We provide a secure data management platform capable of portable cloud-native data analytics delivered in an open, hybrid data platform. Cloudera's product offerings can bring several benefits when implementing a hybrid cloud solution across on-premise and cloud service providers to the tactical edge. Here are some key benefits:

1. **Unified Data Management:** The Cloudera Data Platform (CDP) provides a unified data management solution. It enables seamless integration and management of data across hybrid environments, including cloud providers and edge locations. This unified approach simplifies data ingestion, processing, and governance, ensuring consistent and efficient data management throughout the hybrid architecture.
2. **Data Security and Governance:** Cloudera prioritizes data security and governance. Its products offer comprehensive security features, including NIST-approved data encryption algorithms, RBAC/ABAC, and auditability. Ensuring sensitive data is protected throughout the hybrid cloud solution, addressing security concerns when dealing with critical information in tactical edge environments.
3. **Advanced Analytics and Machine Learning:** Cloudera's platform integrates advanced analytics and machine learning capabilities to empower the warfighter to gain actionable insights and make data-driven decisions, even in resource-constrained tactical edge scenarios.
4. **Data Availability and Real-time Insights:** The platform supports streaming data ingestion, processing, and analysis, enabling organizations to capture and analyze data in real time, even at the tactical edge. This capability facilitates immediate decision-making and enhances operational efficiency.
5. **Seamless Integration with Cloud Providers:** Seamlessly integrate with major cloud providers, including Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP). It enables organizations to leverage cloud-native services while maintaining consistency and interoperability across the hybrid architecture.

Overall, Cloudera's product offerings provide a robust and comprehensive solution for implementing a hybrid cloud architecture from a cloud provider to the tactical edge. They address key challenges such as data management, security, scalability and real-time analytics, enabling organizations to harness the full potential of their data in hybrid environments while ensuring operational efficiency and effectiveness.

**BIO:** James S. Herron (CISSP, CISM, CRISC) is a solution engineer at Cloudera Government Solutions, Inc. (CGSI). As a U.S. Air Force veteran, James has more than 20 years of experience supporting the federal government, intelligence community and Department of Defense.

# I Got 99 Problems, but Compliance Ain't One

**Joe Hagan, Senior Sales Engineer, Splunk** • johagan@splunk.com

## ABSTRACT

With Compliance Essentials for Splunk (CE4S), organizations can now streamline continuous monitoring efforts, improve cybersecurity posture and address the requirements of different National Institute of Standards and Technology (NIST)-based control frameworks, including the following: Risk Management Framework (RMF), Cybersecurity Maturity Model Certification (CMMC), Defense Federal Acquisition Regulation Supplement (DFARS) and the Office of Management (OMB) M-21-31 MEMORANDUM.

CE4S provides turn-key dashboards that align with NIST Cyber Security Framework. Organizations can utilize their existing Splunk infrastructure to provide a low-effort path to operationalizing data for information security compliance visibility.

**BIO:** Joe Hagan is a senior solutions Engineer at Splunk, holding a Masters in cybersecurity from the University of Maryland. Spending the first 5 years of his career in the commercial world, Joe shifted gears and focused the past 15 years on public sector/DoD spaces in a variety of roles and duties. Having first touched Splunk in 2011, attending his first .conf in 2012, Joe fell in love with the product and platform. This passion and obsession lead him to create the query repository website GoSplunk.com, and inevitably join the mothership that is Splunk in early 2019.

# Protecting Hybrid, Multi-Cloud Environments

**John Harmon, RVP, Cyber Solutions, Elastic Federal Cyber Solutions •**

john.harmon@elastic.co

## ABSTRACT

The Army is pursuing a multi-cloud, multi-vendor hybrid approach, enabling its forces to access information anywhere at any time: from servers within data centers, across all types of cloud infrastructures, commercial and private, as well as devices in tactical environments. This means forces must operate, even if systems are disconnected, and be able to communicate with intermittently connected systems, devices and people.

Hybrid and multi-cloud security can be complex, especially since military cloud infrastructures must adhere to U.S. Department of Defense Impact Levels, which categorize information systems and the information they store based on the sensitivity of the information. Moreover, data, which is growing exponentially, is now scattered across multiple environments. IT and security teams often do not have data visibility, making it more difficult to protect. At the same time, different cloud providers have their own security protocols and policies that must be considered as defense agencies develop and implement cloud strategies and solutions.

Another challenge is cost. Pulling data out of one hyperscale cloud infrastructure like Microsoft Azure into Amazon Web Services (AWS), or vice versa, is expensive. Or for that matter, pulling data out of the cloud infrastructures into on-premises environments, which are not going away any time soon, or tactical environments, can be costly. The Army needs solutions to enable its forces to operate securely and protect their assets no matter where they are.

Elastic is the only vendor that can provide security services on prem, in hybrid cloud, multi-cloud and tactical environments, using the same software--cost-effectively. Elastic performs log analytics, full-text search, security intelligence, business analytics and operational intelligence. Our software defends endpoints, collects cybersecurity telemetry data and protects any cloud element, no matter where Army forces and their systems are located. Data is everywhere, which impacts how it is defended, collected, analyzed, and stored. Elastic allows organizations to keep the data where it is generated by creating a data mesh, which unites disparate data sources and links them together through centrally managed data sharing and governance guidelines. As a result, security teams can analyze cybersecurity telemetry data and protect data wherever it resides.

Since the amount of data in a hybrid cloud and multi-cloud environments is huge, Elastic provides a capability called frozen tier with searchable snapshots that lets organizations completely decouple compute from storage and directly search data in object stores such as AWS Simple Storage Service (S3), Microsoft Azure Storage and Google Cloud Storage. This significantly expands an organization's data reach by storing massive amounts of data for the long haul at much lower cost while keeping it fully active and searchable. Defense agencies can store telemetry data for as long as they want, affordably, while staying in compliance with Memorandum 21-31, which describes logs that agencies must capture as well as required retention

times. Having access to telemetry data over the long term increases the DoD's visibility before, during and after a cybersecurity incident.

Ultimately, Elastic focuses on providing defense agencies with the software to serve the mission rather than having the mission serve the software.

**BIO:** John Harmon currently leads the Elastic Federal Cyber Solutions business for the Department of Defense, U.S. intelligence community, federal law enforcement and civilian agency customers. He spent the past 19 years in cybersecurity as a SIGINT analyst, cyber capabilities developer, technical team lead and federal sales leader. He is also an adjunct professor at Georgetown University, where he teaches cybersecurity strategy.

# Multi-orbit, Multi-Link Terminal for Bandwidth Resiliency at the Tactical Edge

**John Lane, Chief Sales Engineer, ALL.SPACE** • [jlane@all.space](mailto:jlane@all.space)

## ABSTRACT

The Army's insatiable bandwidth demand is creating new pressure to embrace a multi-orbit strategy that goes beyond traditional geosynchronous orbit (GEO) satellites to include MEO and LEO constellations.

But orbital diversity in today's contested space environment only works if you have a flexible ground segment that can switch between orbits and provide non-interrupted connectivity. Unfortunately, NGSO constellations like Starlink have already been shown to be vulnerable to jamming by Russia in Ukraine. According to The Washington Post, Russia is using its Tobol electronic warfare systems to disrupt Starlink's transmissions in Ukraine. In addition, Defense One recently reported that Ukrainian troops attributed problems with Starlink on Russian jamming.

However, with ALL.SPACE's new multi-orbit, multi-link terminal designed for defense users, if one network becomes unavailable, you can seamlessly migrate to a new constellation whether it be GEO, MEO or LEO.

ALL.SPACE's SMART terminal, built with defense requirements in mind, isn't just about instantaneous bandwidth. The terminal design allows you to eliminate single points of failure and to have path diversity using multiple satellite systems and multiple links — enabling you to multiply that capacity with each beam.

Commanders can maintain command and control communications, get updates to the common operating picture and get the latest intelligence in the moments that matter to ensure mission success, regardless of whether they are stationary or on the move. If a satellite becomes unavailable, they can seamlessly move to another constellation whether it be commercial or military GEO, or a new MEO or LEO satellite.

We have created a device field proven to hold multiple performance links over multiple satellites simultaneously without losing link performance.

The terminal works over land, sea and air, equipping users with tools to stay connected with greater resiliency and flexibility and the added ability to future-proof their networks — the terminal is independent of any satellite or network, allowing the terminal to be upgraded with additional software-enabled features and functions. With efficient and secure terminal routing, data can travel across multiple links and orbits.

This all-electronic plug-and-play solution eliminates the need for external devices or cables, making installation and maintenance in a conflict zone fast and hassle-free. It uses a single aperture that can transmit and receive multiple signals on different satellites through a patented RF-lens beam-forming technology. ALL.SPACE's electronic steering allows quick direction changes, while intelligent software ensures each independent link can change orbits and networks to avoid interference. Unlike traditional arrays, ALL.SPACE's design uses separate processing channels for each link, enabling independent functionality without interference.



Our SMART terminal's plug-in components, software-defined modems, edge compute modules and intelligent software overlays provide unprecedented flexibility and resilience in the face of evolving threats. The scalability of the terminal design offers new pathways to gather, analyze and disseminate data to better understand what the data means and getting the data where it needs to go quickly.

The modularity and openness of the platform compared with vertically integrated solutions mean that the Army can establish communications through any network or satellite — there is no need to restrict selection of communications options based on which terminal is installed on which platform. Changing to a new network is as simple as clicking a button or swapping a modular modem card into the chassis.

With our terminal's onboard edge compute capability, Army users can reduce bandwidth over the link through caching or aggregation. By processing and analyzing vital information in real-time, edge compute modules enable faster decision-making and improved situational awareness. In addition, intelligent data filtering and prioritization help conserve limited bandwidth resources and ensure the transmission of crucial data.

To conclude, the military's need for always-on bandwidth means it can no longer rely on a single network, satellite or orbit to be effective, especially in the race for space superiority in global conflicts. With ALL.SPACE's SMART terminal, defense users can rely on multi-orbit, multi-link connectivity for a new level of assured communications and agility in the battlefield.

**BIO:** John Lane is chief sales engineer for ALL.SPACE. He supports product development, sales and U.S. government programs. John spent 25+ years supporting PEO C3T's tactical satellite communications efforts. Prior to John's retirement from the government, he was PdM SATCOM's Technical Management Division chief.

# Bringing 5G Capacity, Capabilities to the Battlespace

**Ken Riordan, Principal Architect, Nokia Federal Solutions •**

ken.riordan@nokia.com

## ABSTRACT

Today, modern battlefield networks are increasingly responsible for not only voice communications but large and varied data, including still images, video, sensor data, maps, situational awareness data and inventory information. These networks must gather all that data, send it for analysis by remote compute resources, then distribute the fruits of that analysis back to the battlefield.

Unlike traditional military communications systems built for single channel, voice-based command and control, 5G is designed to provide high-speed data connections to many devices and users simultaneously — it is not solely, or even primarily, about voice communications. It's about acquiring and distributing intelligence, surveillance, and reconnaissance (ISR) data and running applications like the Android Team Awareness Kit (ATAK).

Nokia has developed a suite of product solutions code named “Banshee” in partnership with Fenix Group, Inc. Banshee is an all-in-one 4G/5G network that fits the physical requirements for troops to carry in the battlespace. When Banshee is switched on, it provides 4G/5G coverage for the deployed warfighters to use off-the-shelf smartphones to connect to each other, acquire video feeds from drone-mounted cameras, access ISR data, and monitor the underlying biometrics (heart rate, blood pressure, etc.) of those in the network, among other capabilities.

**BIO:** Ken Riordan is Principal Architect at Nokia Federal Solutions, where he specializes in radio access networks and tactical edge solutions for the U.S. federal government. Prior to joining Nokia, Ken led product management at Loon (an Alphabet company). Loon was a pioneer in High Altitude Platform Station (HAPS) technology, having launched the first commercial HAPS networks. While with Loon, Ken helped form the HAPS Alliance and served as the Alliance's first president. Throughout his career, Ken has developed products for mobile devices and network solutions and worked to launch networks that span the full history of cellular communications standards, including AMPS, GSM, CDMA, WiMAX, LTE and 5G. Ken currently serves on the Executive Committee of the National Spectrum Consortium. He also currently serves as president of the HAPS Alliance. Ken served on the Executive Board of the Small Cell Forum and as Technical Committee chair and Forum vice-chair for the Wireless Innovation Forum. He has been a contributor to 3GPP and has supported regulatory and export control policy development for the Federal Communications Commission and the Department of Commerce. Ken holds a degree in electrical engineering from the Georgia Institute of Technology.

# Bringing 5G AI and Frequency Agile Cognition to the Tactical Edge

**Ken Riordan, Principal Architect, Nokia Federal Solutions** •

ken.riordan@nokia.com

## ABSTRACT

Effective operation of a tactical cellular network on the battlefield necessitates understanding the local electromagnetic environment (EM) and adapting to that environment as mission parameters dictate. Nokia's current suite of tactical edge communication products (codenamed "Banshee") offers significant capabilities to adapt to changing EM requirements. Even greater capabilities are being developed that will bring greater flexibility, resilience against detection, interference, and jamming, combined with capabilities to blend into the local EM landscape — Hide in Plain Sight.

Planned product capabilities include highly flexible, frequency agile, radio architectures that can support operation across up to 1 GHz of radio spectrum and greater than ten separate 3GPP bands in a single product instance. An integrated edge compute engine will take in local real-time EM environmental data, combined with intelligence about the adversary's signal intelligence systems and make real-time cognitive decisions regarding optimal frequency selection.

Additionally, the compute engine will be capable of instructing the radio to perform continuous pseudo-random changes in radio resource assignments (in frequency, time, and space) in a purposeful attempt to thwart the nefarious interests of an adversary.

**BIO:** Ken Riordan is Principal Architect at Nokia Federal Solutions, where he specializes in radio access networks and tactical edge solutions for the U.S. federal government. Prior to joining Nokia, Ken led product management at Loon (an Alphabet company). Loon was a pioneer in High Altitude Platform Station (HAPS) technology, having launched the first commercial HAPS networks. While with Loon, Ken helped form the HAPS Alliance and served as the Alliance's first president. Throughout his career, Ken has developed products for mobile devices and network solutions and worked to launch networks that span the full history of cellular communications standards, including AMPS, GSM, CDMA, WiMAX, LTE and 5G. Ken currently serves on the Executive Committee of the National Spectrum Consortium. He also currently serves as president of the HAPS Alliance. Ken served on the Executive Board of the Small Cell Forum and as Technical Committee chair and Forum vice-chair for the Wireless Innovation Forum. He has been a contributor to 3GPP and has supported regulatory and export control policy development for the Federal Communications Commission and the Department of Commerce. Ken holds a degree in electrical engineering from the Georgia Institute of Technology.

# Hybrid Cloud Solutions — People, Process & Technology

**Kimberly C. Ullmann, Team Lead, Peraton** • kimberly.c.ullmann@peraton.com

## ABSTRACT

Cloud adoption, implementation and migration, while mandated by the DoD and encouraged for fiscal and security advantages, is a significant disruptor for operations and application teams. The challenges are amplified for the tactical-edge.

Through Peraton's operations supporting the U.S. Marine Corps, we execute a hybrid-cloud to help the USMC achieve its goals for rapid migration and centralized command and control capabilities. Our partnership is in the early stages of commercial cloud enablement and migration, although we have operated a private-cloud enterprise-level, primarily PaaS solution, for more than six years. Success in this environment required focus on ensuring our team was ready for cloud technology through training and development. We also worked with the USMC to implement its VMWare Software Defined Data Center technology to enable commercial cloud operations to operate much like the on-prem environment. Finally, Peraton's focus on the process foundations for cloud operations and security supported a successful pilot providing enterprise-hosted cloud capabilities for afloat Marines by ensuring unique technical solutions for tactical edge users could be integrated into the cloud-hosting environment.

Peraton's support to the USMC hybrid, multi-cloud environment is just one example of Peraton's commitment to helping customers achieve cloud objectives. Peraton delivers secure, hybrid multi-cloud capabilities through the CloudOnyx capability suite. CloudOnyx brings foundational business and enterprise IT cloud capabilities including unique connectivity solutions to realize cloud capabilities for the tactical edge, distributed/disadvantaged user client. We partner this with AI and machine learning for data access, visibility and analytics; all enabled by transformation services to make the move to cloud.

**BIO:** Kim Ullmann leads Peraton's team providing operations and security support to the U.S. Marine Corps' enterprise hybrid-cloud hosting environment. The HCS team works with the USMC Enterprise Hosting Management leadership to provide engineering, planning, operations and sustainment support to a fully virtualized datacenter environment on-prem while building and migrating to hybrid-cloud hosting capabilities in both AWS and Azure IL6 environments. In addition, the team provides cybersecurity support for vulnerability management, self-assessment and audit and Independent Verification and Validation of on-prem and cloud infrastructure as well as enterprise hosted applications.

Prior to joining Peraton, Kim served as the U.S. Postal Service Office of Inspector General (OIG) as cloud architect and chief information security officer, planning the OIG's initial cloud implementation primarily into Azure Gov Cloud, and prior to that, establishing the OIG's first Security Operations Center. Kim retired from the U.S. Air Force after serving in a variety of cybersecurity and network operations positions, including Joint Staff J6 Cybersecurity Division Chief during the planning and designation of Cyber Command and Commander of the 83d Communications Squadron responsible for consolidating network operations and security capabilities for five USAF major commands into a single command and control organization.

Kim holds Master's Degrees in information resource management (Air Force Institute of Technology), military operational arts from Air University and national resource strategy from the National Defense University.

# Providing Service Views for C2 Situational Awareness

Lee D. Koepping, Chief Technologist, ScienceLogic • lkoepping@sciencelogic.com

## ABSTRACT

Command and control (C2) situational awareness is essential for the Army IT support staff and commanders to effectively perform their duties. Service or mission aligned views play a vital role in correlating data and information from multiple sources to present a unified view of the operational environment. This allows the support staff to quickly identify and understand threats, assess the situation, and make informed decisions — accurately, timely and ultimately automate repetitive responses and restoration capabilities.

Service views are typically created by aggregating data from different sources, such as sensors, systems and databases. The data is then filtered, processed and analyzed to identify patterns and relationships. This information is then presented to the support staff in a way that is easy to understand and visualize.

Service views can be used to support a variety of C2 tasks, such as:

- Monitoring the operational environment: Service views can track the status of assets, identify threats, and assess the overall situation.
- Planning and executing operations: Service views can develop plans, track the progress of operations, and identify opportunities for improvement.
- Responding to incidents: Service views can identify and understand incidents, assess the impact and develop a response plan, or in many cases, automate the initial triage or restoration of critical IT elements.

Traditional IT monitoring platforms lack the capabilities to reflect information technology as a true service aligned to the mission, many organizations have visibility to the parts but not a true end-to-end view of the service being provided. Additionally, the ability to support services is made more difficult in having a myriad of tools supporting separate technologies and not reflecting the context of how they work together to provide a services or multiple services, especially across shared environments.

ScienceLogic is a platform that helps improve access to digital services by providing comprehensive monitoring and management capabilities for complex IT estates. The platform enables IT teams to monitor and manage the health and performance of digital services and underlying infrastructure components, including applications, servers, storage, network devices, and cloud services and organize into a mission aligned view that adds context to visualization, correlation, and automation. By analyzing data from multiple sources, including log files, network traffic, and application performance metrics, support teams can make informed decisions about resource allocation, capacity planning, and optimization.

Service views are a powerful tool that can help the Army IT support staff to improve C2 situational awareness. By correlating data from multiple sources and presenting it in a way that is easy to understand, service or mission views can help the support staff to make better decisions and improve the overall effectiveness of their mission operations.

**BIO:** Lee Koepping is a seasoned executive and technical leader with more than 30 years of experience in IT engineering, technical solutions sales, project and business management for federal and commercial enterprises. Lee is the Chief Technologist for ScienceLogic, supporting the public sector marketplace, focused on providing leadership and coordination of the company's technical direction and establishing the go-to market strategy and technology portfolio to provide government and DoD organizations comprehensive solutions to the challenges faced in the modern technology landscape. Lee began his career in the U.S. Navy, where he received his formal education in electronics engineering and worked in naval intelligence joining the IT industry following 8 years of decorated service.

# Achieving a Unified Hybrid Cloud Through Model-Driven DevOps

**Lee Van Ginkel, Team Leader - Federal Platforms and Automation, Cisco •**

lvangink@cisco.com

## ABSTRACT

As the Army expands cloud usage for tactical edge services, reliable transport becomes crucial. The service can achieve a unified hybrid cloud through implementing Model-Driven DevOps. Model-driven DevOps treats infrastructure as software, applying cloud operations practices to network management. This approach allows for the reuse of existing application management tools and processes, simplifying operations. To further streamline operations, we translate vendor-specific CLI commands into a standardized, vendor-agnostic data model, allowing operators to deploy services consistently and predictably, regardless of the underlying hardware. Model-Driven DEVOPS is a framework that provides the foundation for automation and is not reliant on specific tools. This approach gives customers full control of their data, as we focus primarily on making that data easier to manage and operate.

Implementing model-driven DevOps can be done in phases:

- **Onboarding:** The onboarding process involves programmatically collecting and centralizing configurations from all devices to create a source-of-truth. Configurations are stored as Infrastructure as Code (IaC) using Ansible and API normalization tooling. Standardizing communication with a common API across vendor platforms is vital for scaling automation and standardizing operations.
- **Data Normalization:** Harvested data undergoes normalization using an OpenConfig service package to standardize the data model across vendor platforms. The source-of-truth is presented to operators in a human-readable file structure, organized based on the customer's hierarchy. To minimize redundancy, common functions are elevated within the hierarchy, allowing shared services to be defined once and applied to devices with specific tags.
- **Continuous Integration:** Data is processed through source control management tools like GitLab to enforce governance and movement. A simulated digital twin of the customer's infrastructure is created through continuous integration, where changes are tested. Model-driven DEVOPS Ansible collection includes pre-built validation and checks executed within the pipeline.
- **Validation:** JSON Schema validates the data against predefined rules, including STIG schemas or common standards, before deploying configurations to devices. The benefit of this approach is the large library of existing schemas that can be shared or re-used across agencies.
- **State Checking:** After validation, data is pushed into the digital twin for additional state checks. This ensures proposed changes have the desired effect without disruptions, reducing risk through simulation.
- **Continuous Deployment:** Approved changes are deployed into the production environment only after thorough review and approval processes.



By adopting mode-driven DevOps, we establish a framework for collaboration and automation throughout the network lifecycle. This includes development, testing, deployment and ongoing maintenance. The key principles of DEVOPS, such as continuous integration, continuous delivery, and infrastructure as code, enable us to streamline operations and achieve greater scalability and efficiency, while truly providing a unified operating model.

**BIO:** Lee Van Ginkel is a seasoned Cisco professional with 14 years of experience, currently leading a team supporting the Navy. In his career, he worked on cloud migration and cyber projects for Homeland Security and other civilian agencies, focusing on network and security automation. He also helped implement DevOps for immigration digitization and designed the IRS's network segmentation architecture for compliance and security audits. Now, Lee concentrates on improving how his company delivers capabilities to federal customers, using Infrastructure as Code and DevSecOps. He is actively involved in implementing a vendor-agnostic Infrastructure CI/CD pipeline for the Navy to boost automation and compliance. Lee holds a Master's in cybersecurity from Brown and a Bachelor's in information systems from the University of Maryland.

# Leveraging Army Investments in VMWare Technologies to Meet Target Level Zero Trust and the Path to Advanced ZT

**Leo Lebel, Senior Solutions Architect**

**Chris Lewis, Sr. Account Executive, Network and Security, Federal**

**James Emmons, Networking & Security Specialist Account Executive, VMware** • lew-isc@vmware.com

## ABSTRACT

VMware's suite of products, including NSX, Threat Prevention and Multi-Cloud services, all with a zero-trust focus, offer a comprehensive solution to address the defined problems.

**Bandwidth Limitations:** VMware NSX optimizes network performance and bandwidth utilization with its software-defined networking (SDN) capabilities. Through smart routing, prioritization and network virtualization, NSX ensures the efficient use and management of available bandwidth, thereby reducing the limitations at the tactical edge.

**Hybrid Cloud Solutions:** VMware's multi-cloud services leverage the power of VMware Cloud Foundation to simplify the deployment and operation of a hybrid cloud. This facilitates seamless and secure data exchange between cloud environments (Army, commercial or private) and the tactical edge, offering benefits like scalability, resilience, and efficient resource utilization.

**Converged Data Transport:** VMware NSX provides a secure, efficient and cost-effective solution for the transport of converged data. By leveraging a software-defined approach, NSX enables secure machine-to-machine data exchanges integral to C5ISR/EW systems. The zero-trust model ensures only authenticated and authorized entities can access and communicate within the network, contributing to security.

**Tactical Edge:** VMware's solutions are built to deliver high performance even on small form factor devices at the tactical edge. Integrating AI/ML capabilities, they can execute cognitive weaponizing tasks for EW using ES operational information, enhancing the operational effectiveness and decision-making process.

**Dynamic Spectrum:** VMware NSX allows for dynamic management and allocation of network resources, including spectrum access. Through the use of SDN, it can support real-time adjustments to network configurations, ensuring robust EMS-dependent capabilities even in contested and congested environments.

**Risk and Opportunity Correlation:** VMware's Threat Prevention platform utilizes AI/ML algorithms to correlate data and inform of emerging risks and opportunities. This capability aids commanders in making timely and data-driven decisions to ensure the success of ongoing missions.

**Cyberspace Social Layer:** Leveraging zero-trust principles, VMware's suite can create a cyberspace social layer that effectively identifies and correlates actors, units, activities and affiliations. These insights can then be incorporated into the common operating picture (COP) and military decision-making process (MDMP) products, promoting situational awareness and informed decision-making.

**BIO:** Leo Lebel is a Senior Solutions Architect for VMware with more than 28 years of IT and cyber security experience. He is also a retired Marine cyber information systems security officer. He has a Bachelor of Science degree in information technology and several industry certifications from Cisco, CompTIA, Fortinet, ISC2, Microsoft, ITIL and also serves as a certified Provisional Assessor for the Department of Defense's Cyber Security Maturity Model Certification (CMMC) (Cyber AB) program.

Chris Lewis is a retired Army signal warrant officer with more than three decades of combined military and civilian IT experience. He served in Desert Shield/Storm, Operation Enduring Freedom and Operation Inherent Resolve with conventional and SOF elements. He has been with VMware for 7 years with a focus on network and security, most recently supporting Army, Defense Agency, SOF and COCOMS.

James Emmons is a Networking & Security Specialist Account Executive for VMware with more than 25 years of technology and cybersecurity experience. James has been involved with zero trust and multi-cloud strategies at VMware for approximately 8 years. He is a disabled Marine Corps veteran with Master's & Bachelor's degree in networking management. He has several industry certifications from VMware, Cisco, CompTIA, NetApp, Microsoft & ITIL. Currently, James is completing his Master's degree in cybersecurity management that is certified from the National Security Agency and the Department of Homeland Security.

# NetApp ONTAP: A Simple, Flexible Solution for AI at the Edge as a Hybrid Cloud Solution

**Mario LaNasa, Senior Solutions Engineering Manager**

**Matt Dawson, District Sales Manager, NetApp** • [mario.lanasa@netapp.com](mailto:mario.lanasa@netapp.com)

## ABSTRACT

With this hybrid cloud infrastructure, NetApp ONTAP Select (Software Defined Storage) acts as a powerful AI inference server, with ONTAP AI creating the trained model. After you train a model, you can deploy it to perform inference workloads. With NetApp FlexCache caching, your data scientists can access the trained model without exporting the full model, improving performance and ease of use. When the inference model is deployed, results can be fed back into the training model to improve deep learning.

In edge environments, NetApp provides important benefits that a traditional infrastructure model does not, including:

- Independent scaling. Maximize your resources and minimize the hypervisor tax. Grow your IT based on your needs, not architectural deficiencies.
- Workload consolidation. No more silos, no more unnatural workload constraints. Achieve more secure data, better QoS, dedicated performance and guaranteed service levels.
- Open hybrid multi-cloud. No cloud lock-in. You get consistent IT consumption across public cloud, government cloud, IL5/6, private cloud, and on-premises environments.
- Guaranteed 4:1 efficiency. Get the industry's most effective storage efficiency guarantee, with no impact on your system performance.
- Security. Data is protected in flight with snapmirror AES-256 level encryption and protected at rest with volume and aggregate level encryption.
- Support for Delayed/Disconnected, Intermittently Connected, Low-Bandwidth (DIL) Communications. NetApp SnapMirror intelligently only moves changed blocks based upon last sync.

**BIO:** Mario LaNasa joined NetApp in 2011 and is currently a senior solutions engineering manager for the DoD. Mario has more than 20 years of engineering and technical sales experience supporting a variety of public sector as well as commercial customers. Mario has focused on Data Management and Security for more than 20 years, including on-premises, hybrid and cloud technologies. He has a passion of teaming with customers, partners and colleagues to drive great outcomes to win.

Matt Dawson is the Director of Army Sales, responsible for NetApp's total Army business and strategy. With more than 17 years of leading and delivering operational readiness initiatives to the DoD, Matt has held vital roles at NetApp, to include leading the SOCOM and COCOM business as district manager and sales rep. He has a deep understanding of the Army's digital enterprise and has successfully partnered his team with Army organizations and programs to usher in the most cutting-edge technology for data storage and hybrid/multi-cloud data management solutions.

# Empowering the Edge with Event Streaming

Michael Peacock, Staff Solutions Engineer, Confluent • mpeacock@confluent.io

## ABSTRACT

The Army has a strong desire to become a data-centric agency. This is a clear strategy that is described by all levels within the chain of command. The awareness of the importance of data and its role as a strategic asset is a critical driver of the overall roadmap across the Army Enterprise. Within that roadmap is the requirement that mission-critical data be interoperable and accessible for all strategic and tactical programs, including disrupted, disconnected, intermittent and low-bandwidth (DDIL), tactical edge, and enterprise cloud environments. An emerging approach to becoming data-centric is to treat data as a first-class citizen within an enterprise and migrate to a data mesh strategy.

A properly implemented data mesh can bring rigor to the Army's data practices, introducing the means to access and use important data across the Army Enterprise. It enables scalability of the data architecture both technologically and organizationally, eliminating ad hoc point-to-point connections in data pipelines. A data mesh brings selected mission data to the forefront, exposing it as a first-class citizen for systems and processes to react on directly.

The "Edge" is an ambiguous term used to describe a variety of deployments not at the center of a data enterprise. It could be a small IoT device, or a full-fledged mobile data center deployed strategically. Getting data from that edge to the centralized location supports critical mission requirements. Through a data in motion approach, organizations can tap into data streams that are continually evolving and flowing from a growing network of edge devices and systems. This session will describe how Confluent uses the various tools to support the edge and hybrid solutions.

**BIO:** Mike Peacock has more than 20 years of experience leading new business activities and developing and designing high-available, real-time, mission-critical software across various public sector programs. As a Federal Solutions Engineer at Confluent, Mike works directly with multiple organizations within the DoD (public sector) to understand their architecture, and recommend solutions to modernize and implement advanced technologies in the areas of real-time event streaming, cyber/SIEM solutions, AI/ML, edge computing, and cloud migration strategies.

# Providing a High-Bandwidth, Low-Latency Symmetric Communications Solution

**Peter Ford, EVP, Government Operations, QuSecure** • [pete@qusecure.com](mailto:pete@qusecure.com)

## ABSTRACT

The QuProtect™ software is designed to protect data — commercial and government — from quantum and classical cybersecurity threats throughout the data lifecycle. Our end-to-end solution powers an easy transition to quantum-resilience to protect digital assets and data, wherever they reside on the network. We combine a robust QRNG with NIST-approved PQC algorithms to create the strongest PQC currently available. This combination is used by the orchestration platform to provide a high-bandwidth, low-latency symmetric communications solution compatible with both pre/non-quantum and quantum-enabled systems. In addition, this PQC capability can be deployed via software across all network devices to securely transport QRNG-enabled symmetric keys to legacy satellites or IoT devices to establish secure communications.

Our PQC solution is being considered by some of the largest IT providers in the United States within their cloud-based products and services. They are doing so in recognition of the devastating impact that collect-now, decrypt-later (CN DL) attacks will have on our markets and national security.

**BIO:** Pete Ford has decades of experience in executive roles at Raytheon and Northrop Grumman, and Lawrence Livermore National Laboratory. He specializes in advanced aviation and space integration, communication protocols, WMD counterproliferation & advanced threat developments. Pete is also a distinguished retired colonel and fighter pilot commander from the U.S. Air Force.

# Helping the Army Create a Data Centric Fabric While Consolidating and Streamlining the Enterprise and Tactical Networks

**Rich Gleason, New Business Proposals, Huntington Ingalls Mission Technologies** • frederick.gleason@hii-tsd.com

## ABSTRACT

The Army's goal is to create a data centric fabric while consolidating and streamlining the enterprise and tactical networks. Some of the main obstacles are the size and complexity of required objects, the network reliability in a contested environment and the ability of the software to get the right message to the right person at the right time to be useful and effective. Huntington Ingalls Mission Technologies addresses needs and challenges of the Army Operational View, and provides options for the following topics:

- The fragility of the network, threats and options
- Integrated comms
- The data fabric
- Working across echelons
- Edge devices
- End-to-end zero trust
- The need for a common operating picture (COP) stretched for the integration of the enterprise and tactical networks.

**BIO:** Rich Gleason is part of Huntington Ingalls Mission Technologies new business team with a concentration on solutions development. He and the team have been very involved in advanced technologies offered through the research labs for Army, Navy and Air Force and have been evaluating current Army technology practices.



# Leveraging Cisco Soft Client on ATAK with Cisco Communications Manager: An Abstract Response

**Robert Alred, Technical Solutions Architect, Cisco** • roalred@cisco.com

## ABSTRACT

This abstract provides an overview of the potential benefits and implications of integrating Cisco Soft client for Mobile with the Android Team Awareness Kit (ATAK) and Cisco Communications Manager (CUCM). The objective is to explore the advantages of this integration in enabling effective communication and collaboration in tactical edge environments.

The integration of Cisco's soft client on ATAK with CUCM presents a unique opportunity for the Army. By combining the capabilities of these platforms, users gain access to a comprehensive suite of communication tools, including voice, video, chat, presence, and file sharing.

One of the key advantages of this integration is the ability to extend Cisco Communications Manager features and services to mobile devices running ATAK. This integration empowers users to communicate seamlessly across devices, bridging the gap between the tactical edge and command centers. It facilitates real-time situational awareness, allowing personnel to make informed decisions and coordinate operations effectively.

Moreover, the integration offers interoperability with existing tactical communication systems, enhancing the overall connectivity and collaboration among team members. By leveraging Cisco Jabber for Mobile on ATAK with CUCM, personnel can communicate securely and reliably using military-grade encryption and authentication protocols. This ensures the confidentiality, integrity, and availability of critical communications.

Additionally, the integration enables enhanced information sharing and coordination through the integration of ATAK's mapping, tracking, and geospatial capabilities with Cisco's communication features. Personnel can share location data, images, videos, and other relevant information in real-time, enabling a shared operational picture and improved situational awareness.

In conclusion, the integration of Cisco soft client on ATAK with Cisco Communications Manager offers a powerful solution for enhancing communication and collaboration in tactical edge environments. By enabling seamless interoperability, real-time situational awareness, and secure information sharing, this integration can significantly improve operational effectiveness for military and emergency response personnel.

**BIO:** Robert Alred is a highly experienced Cisco Technical Solutions Architect with more than 30 years of expertise in communications and networking. After leaving the U.S. Navy, he embarked on a successful career, specializing in designing and implementing advanced solutions for diverse industries. With a deep understanding of technology and a strategic mindset, Robert has become a trusted expert in creating robust network infrastructures that drive operational efficiency and support organizational growth.

# Bandwidth Limitations

**Rohit Bhanot, Vice President, JMA Wireless** • rbhanot@JMAWireless.com

## ABSTRACT

Bandwidth limitations significantly hinder our ability to push, receive and analyze information at the tactical edge; how does your technology address this issue?

In an era of increasingly complex threats, military operations demand enhanced connectivity, real-time data processing and secure and reliable communication networks at the extreme and tactical edge. 5G offers the potential to address these requirements by overcoming the bandwidth constraint and provide warfighters with a distinct advantage in the field.

Furthermore, the high data rates and low latency of 5G networks enable real-time communication and processing of critical information. This capability allows warfighters to access and analyze data-intensive applications such as augmented reality, virtual reality and artificial intelligence algorithms at the tactical edge. Rapid data transfer and low latency empower warfighters with actionable intelligence, enabling them to respond swiftly to dynamic battlefield conditions and gain a tactical edge over adversaries.

JMA Wireless, a global wireless leader in 5G and 5G ORAN in partnership with Sherpa 6, successfully demonstrated on September 14, 2022, at that 5G mobile capabilities can increase operational and tactical efficiency for soldiers on the frontlines. The demonstration was a daylong event at a Sherpa 6 facility near Fort Bragg, NC, showcasing various military applications and programs over JMA's 5G standalone wireless system connected to the U.S. Army's Integrated Tactical Network (ITN). Under the direction of Dr. Dilip Guha, Director of 5G Tactical Applications for OUSD R&E, Sherpa 6, Inc. (Sherpa 6) led the design, integration, and testing of a private 5G mobile network showcasing tactical edge applications for US armed servicemembers.

This abstract highlights why the integration of 5G technology at the tactical edge is crucial for the success of the warfighter and how the DoD as a whole also stands to benefit from the adoption of 5G technology. The deployment of 5G networks can optimize logistical operations, enhance supply chain management, and improve maintenance processes.

**BIO:** Rohit Bhanot is a federal and DoD-focused strategic business leader. Rohit has spent the last 20+ years in the telecommunications industry with global experience across multiple disciplines, such as sales, business development, services, operations, consulting and strategy. Rohit has had tremendous success in new growth markets, navigating complexity, formulating go-to-market strategies, consultative selling, driving and managing positive change, and building solutions and teams to achieve measured success.

Rohit currently heads up the strategic go-to-market alliances and partnerships program for the DoD space at JMA Wireless with specific focus on 5G Private and Private Hybrid Networks.

Prior to joining JMA Wireless, Rohit held leadership positions at Ericsson and Nokia, Motorola, Alcatel Lucent and Accenture.

# Tactical Data Operations

**Ron Nixon, CTO & CISO, Federal Organization, Cohesity** • ron.nixon@cohesity.com

## ABSTRACT

Information has always been the key to success, on and off the battlefield. But that success depends on having that information available at the right place at the right time. The transition to a “digital force” has data production and consumption growing at exponential rates. This showcase takes the nuances and challenges of battlefield data management into account as we will present practical solutions to meet tactical DataOps requirements.

**BIO:** Ron Nixon is a 23-year U.S. Army veteran with more than 20 years of IT and cybersecurity experience in senior technical management roles. He retired as the senior warrant/CTO for operations at Army Cyber Command, with direct global support to 1.4 million users in strategic and tactical environments. He is currently the CTO and CISO of the federal organization at Cohesity.

# Heightened, Accelerated Performance at the Tactical Edge

**Russel Davis, Chief Operating Officer and Chief Product Officer, Vcinity, Inc.** • rda-vis@vcinity.io

## ABSTRACT

Today, agencies face numerous challenges to securely access, analyze and disseminate massive amounts of ever-growing data from a broad range of sensors and systems. Agencies struggle to securely curate geographically dispersed data repositories for mission-critical analysis, which hinders their ability to meet both the current and projected government stipulated requirements as well as achieve optimal mission results.

Current methods of moving data to disparate locations are hindered by latency as well as bandwidth limitations — stifling an organization's ability to meet mission requirements and deliver results. To pave a future that heightens the capabilities and utilization of the tactical edge, organizations must first re-think the way they move and access their data.

The Edge Access Solution, powered by Vcinity and Dell Technologies, establishes a connective layer to allow compute engines to access data, no matter where it is. This gives organizations options for how they want to use their data (securely and at scale): one, to move the data more efficiently and extremely fast across great distance to where it's needed — or two, to extend the reach of a user or an application to the data wherein it can be computed on without having to be moved first. How does this change an organization's ability to push, receive and analyze information at the tactical edge? With the Edge Access Solution (EAS), data locality is no longer a hurdle to analytics, operations, and innovation.

This abstract touches on how organizations — ones that need the right data in the right place at the right time — can mitigate the effects of latency and maximize your available networks (so you use, on average, 90% or more of your bandwidth for data on a sustained basis) to enabling you to deliver data, more quickly, more efficiently and more securely to the people who need it.

Beyond peeking into how Vcinity and Dell Technologies' EAS minimizes the effects of latency and bandwidth limitations, this abstract discusses the benefits of utilizing EAS and how EAS enhances the mission's ability to push, receive, and analyze more information at the tactical edge. This includes:

- **Extend the Core to the Edge:** By making remote site data accessible with a local-like experience when operating on remote data and begin to work on that data almost instantly.
- **Push data to the Edge:** By creating a pipeline with optimized bandwidth, you can simultaneously move more critical mission data to the tactical edge at unprecedented speeds.
- **Unlock Edge data and bring it to the Core:** By bringing data back to the core at unprecedented speeds with predictable, reliable and secure performance, you can begin timely analysis, enabling you to provide sound (and up to date) recommendations to guide intelligent action.

- Enable write caching and write back performance at the Edge: By delivering high quality, high performance write-caching and write-back at the edge over your existing WAN connections, EAS enables you to protect your existing network infrastructure investments and reduce future network costs.
- Create a data ecosystem with instant access to data anywhere, securely: By extending the core and requiring no changes to your existing infrastructure, EAS delivers the benefits of Dell's PowerScale Solution—anywhere your data and operations exist.
- Uphold compliance requirements with no interruptions to workflow: By creating an intelligent data mesh between core and edge sites, you can maximize operational efficiency.

With the Vcinity and Dell Technologies' Edge Access Solution, agencies can rest assured that their data is safe, reliable, and, most of all, accessible. Now you can get the data you need, at scale, where you need, when you need it — regardless of prior latency limitations or distance. The Edge Access solution gives you the power of the right data, at the right time, to make mission-critical decisions.

**BIO:** Russel Davis brings more than 25 years' experience in management, operational and technical leadership at organizations ranging from start-ups to Fortune 500 companies.

Prior to joining Vcinity, Russel was co-founder and COO of a well-funded venture that developed telecommunications hardware and the service platform managing NFC devices and transactions for transportation and payment systems. He also served as CTO and VP of product development for CIC (a public company) and director of services for Everex Systems (acquired by FPG), as well as working in field services engineering management at Centel Information Systems (acquired by Sprint) and for the U.S. Navy.

# Semantic Search & Sentiment Analysis (Se3An) — High-Definition Mapping of the Information Environment

**Stefano Feijoo, Data Scientist, Peraton** • stefano.feijoo@peraton.com

## ABSTRACT

Effective decision-making relies on continuous observation, gathering of relevant information and rational analysis to make informed choices. The ability to monitor the information environment (IE), including traditional media outlets, social media, websites, blogs, forums and various other means of communication, enables organizations to stay ahead of emerging trends and make timely, data-driven decisions. The capability to perform precise granular sentiment analysis and topic modeling can aid commanders in areas such as campaign evaluation, understanding public opinion, gauging population perception, and conducting adversary analysis.

However, most data channels generate text-based sources, posing challenges for scalable analysis. Previous Deep Learning (DL) and Natural Language Processing (NLP) techniques may yield inaccurate results without extensive labeled training data and human supervision. Moreover, they can produce incorrect answers when performing semantic based data extraction tasks such as question-answering, entity/aspect detection, sentiment analysis and text summarization. By addressing these challenges, decision-makers can benefit from enhanced knowledge discovery, improved assessments, and being well informed in an increasingly information-driven world.

### Solution

Se3An (Semantic Search & Sentiment Analysis) is an innovative application that brings together the power of advanced NLP and Generative AI techniques. With its four distinct sections, Se3An offers a platform where users can delve into their own datasets or tap into Se3An's centralized data sources to conduct a range of tasks. What sets Se3An apart is its ability to provide high-resolution maps of the IE by combining file question-answering, aspect-based sentiment analysis (ABSA), topic modeling, and topic and sentiment longitudinal analysis. All in a minimal or fully unsupervised manner.

The file question-answering section leverages the prowess of fine-tuned Large Language Models (LLMs) such as MPT-30B/7B and Falcon 40B/7B. Users can effortlessly load multiple PDF files and pose questions about their data. With a deep understanding of instructions and context, these LLMs excel in delivering comprehensive and insightful answers.

ABSA takes sentiment analysis to new heights. By harnessing LLMs' superior sentiment understanding, advanced Named Entity Recognition (NER), and Parts-of-Speech understanding, Se3An enables highly granular aspect-based sentiment analysis. It goes beyond simplistic sentiment analysis approaches, providing a nuanced understanding of sentiments expressed towards specific aspects or targets within a text.

Topic modeling in Se3An is elevated by the integration of ABSA. Aspects extracted during ABSA are utilized in creating topic clusters using the BERTopic algorithm. With the application of dimensionality reduction and clustering techniques, Se3An generates topic clusters with high precision. These clusters are enriched with sentiment information per aspect, offering a detailed and high-definition topic mapping of any number of documents.

Finally, Se3An empowers users with topic and sentiment longitudinal analysis. By tracking topic clusters over time, Se3An uncovers trends in topic variability, allowing users to understand how topics evolve and gain insights into shifting priorities or interests. Additionally, sentiment trend analysis per topic provides a comprehensive view of changing sentiment patterns, unveiling the dynamics of emotions associated with different topics over time.

Se3An is a platform that opens new avenues for data exploration and understanding. It is an integrated platform that provides a rich and multidimensional exploration of data. Furthermore, it improves upon previous machine learning techniques by providing better results without the need for training data in a semi-supervised or fully unsupervised manner. With its unique blend of semantic search, file question-answering, ABSA, topic modeling, and topic and sentiment longitudinal analysis, Se3An can reveal insights that were previously hidden enabling data-driven decision-making with enhanced precision and clarity.

**BIO:** Stefano Feijoo is a Data Scientist and part of Peraton's CENTCOM J39 Assessments Team. Based directly on-site, he collaborates closely with clients to transform theoretical concepts into practical solutions. With expertise in software development for Machine Learning, data analysis, and visualization, Stefano plays a pivotal role in driving innovation and delivering effective tools.

Prior to joining Peraton, Stefano held a position at Los Alamos National Laboratory, where he contributed to the success of the Physical Chemistry and Applied Spectroscopy Group. In this role, he supported the software development team by constructing machine learning models, optimizing algorithms, and creating insightful data visualization dashboards.

Stefano holds a Master's Degree in applied physics from the University of Oregon, complemented by a Bachelor's Degree in physics from the Georgia Institute of Technology. His strong academic foundation enhances his ability to excel in complex data-driven projects and contribute to cutting-edge research and development efforts.



# Firmware Under Fire? A Critical Gap in Cybersecurity Programs

Stephen “Steve” Spry, Founder, Spry Squared, Inc. • [steve@sprysquared.com](mailto:steve@sprysquared.com)

## ABSTRACT

Cybersecurity attacks on critical infrastructure is on the rise, with the Colonial Oil Pipeline, Oldsmar Florida Water Treatment Plant, JBS Foods, Israeli water systems, the Ukraine Power Grid, SCADA system of New York’s Bowman Dam as just a few examples. While some were more damaging than others, it does speak to the cybersecurity vulnerabilities of critical infrastructure.

Why is Firmware an Attractive Target? Firmware is on every IT, OT and IoT device. It sits below the OS controlling functions above it. Firmware is not actively monitored for malicious code like other software or operating systems. And your traditional cybersecurity tools like McAfee, Symantec, Tenable, Dragos, etc. DO NOT review firmware for malicious code. An adversary can get in and gain access to firmware without the organization even knowing whether through a cyber-attack or through the supply chain.

Adversaries are aware of this cybersecurity gap and ramping up their attacks on malicious firmware implants, backdoors, etc. Just look at some recent discoveries in Gigabytes motherboards, ASUS motherboards and the recent attack on MSI where adversaries captured copies of the original source code for firmware and BIOS plus the security keys.

From an adversary’s perspective, firmware presents an unusually high-value and strategic target. Firmware exploits give adversaries:

- **The Highest Levels of Privilege:** By controlling firmware, attackers can subvert the kernel and escalate to the highest levels of privilege on the device.
- **A Bypass of Traditional Security:** Attackers can avoid security measures running at the OS and virtual machine layers by controlling how a system boots.
- **Ready-Made Persistence:** Malicious code in firmware is tied to the hardware of the device and can allow an attacker’s code to persist even across a full re-imaging of the system.
- **Stealth:** Compromised firmware enables attackers to perform critical attack functions without detection. Attackers have used out-of-band management features in BMCs and laptop chipsets as a command-and-control channel to evade host-based firewalls.

**BIO:** Stephen “Steve” Spry is a globally recognized information technology (IT) and business leader known for crafting strategic visions to achieve business, IT and cybersecurity goals.

Stephen offers more than 35 years of demonstrated IT knowledge, including more than 20 years of senior management experience in cybersecurity, IT architecture, software development, implementation, support, project management, system and strategic planning. Stephen regularly solves complex cybersecurity and technology challenges in the IT, IoT and OT realms. He is helping to secure critical infrastructure by helping to educate IT/IoT/OT users and secure devices from malicious firmware attacks by adversaries. Stephen has worked in the critical infrastructure areas, including telecommunications, utilities (electric/nuclear) and oil & gas most of his career..

Eight years ago, he founded Spry Squared, Inc., with his wife, Linda Spry. Spry Squared is a minority- and woman-owned small business headquartered in Colorado Springs, Colorado, with offices across the United States. Spry Squared is an experienced federal government and commercial service provider with security cleared personnel working on various projects across the nation. Spry Squared provides organizations with Best-in-Class Cybersecurity Solutions, Vulnerability Management, Enterprise Solutions, Managed IT Services, IT Professional Services, Recruiting Services, Project/Program Management, and technology products.

# Leveraging Virtualization Combined With NSA-Vetted, Pre-Engineered, Scalable Hybrid Infrastructure to Achieve Secure and Flexible Operations

**Therman Farley, Vice President, Information Solutions Group,  
Trace Systems, Inc. • [tfarley@tracesystems.com](mailto:tfarley@tracesystems.com)**

## ABSTRACT

Recent global events have underscored the urgent need for secure, versatile hybrid cloud solutions in military operations. Cybersecurity risks associated with legacy, non-adaptive infrastructure have become increasingly evident. By leveraging virtualization combined with our NSA-vetted, pre-engineered, scalable hybrid infrastructure, the Army can achieve secure and flexible operations.

Implementation of a modular, dynamic, secure hybrid cloud solution to the tactical edge provides a robust and versatile capability for hosting multiple virtual classified workloads securely. Such a solution ensures a ready-to-deploy infrastructure that adheres to stringent DoD & NSA cybersecurity standards, giving operators and security managers alike confidence in the confidentiality, integrity and availability of these mission-critical systems. With scalability and diverse form factors, our solutions meet requirements for enterprise and tactical edge environments while mitigating vulnerabilities.

By deploying this standardized solution across Army echelons, a resilient capability is established to create and geographically distribute multiple secure processing environments within each physical stack. These environments can seamlessly integrate tactical and enterprise services, and enterprise-grade local compute resources enables secure operations in contested and DDIL environments. Our solution's dynamic, easy-to-operate virtualization capabilities, combined with its scalable and compact design, bolster warfighter agility and operational effectiveness while safeguarding against cybersecurity threats.

**BIO:** Therman Farley has served as Trace Systems' Vice President of the Information Solutions Group (ISG) since January 2018. Therman oversees all aspects of the ISG, including financial management, governance, strategic direction, development of the business strategy, as well as oversight for all information systems, innovation, product development and operations. He is a proven leader with significant experience in strategic planning and leading diverse business development efforts and growth opportunities. He is well-versed in emerging technologies and contract and teaming agreement negotiations.

Prior to joining Trace, Therman served as the network operations manager at SAIC in Stuttgart, Germany, providing managerial, technical, functional, supervisory and operational expertise in support of the DoD's wide area network. He further managed network operations, transport and IP in the Theater Networks Operations Center. Therman has served as the chief of Transmissions Network Services Division for the DoD, where he developed, established and maintained strategic business methodology in support of 40+ DISA Europe programs valued at more than \$300 million. He further acted as the European lead for the agency-wide Global Information Grid (GIG) Service Management effort, a \$4.6 billion program.

Therman has a BS in history from the University of South Carolina–Aiken and served 22 years in the U.S. Army, retiring as a major. He is a highly experienced former Army signal officer, with proven ability to manage geographically disparate teams, programs, costs, schedules, risk, resources, and performance on multi-hundred-million-dollar information technology programs on a global level. Therman's professional certifications include Program Management Professional (PMP) (2005) and Information Technology Infrastructure Library (ITIL) v3 Foundations (2008).

# Meeting the Critical Need for a Compact, Secure, Versatile Tactical Edge Processing Capability

**Therman Farley, Vice President, Information Solutions Group,  
Trace Systems, Inc. • [tfarley@tracesystems.com](mailto:tfarley@tracesystems.com)**

## ABSTRACT

Our NSA-vetted tactical edge processing solution addresses this small form factor challenge by offering a compact capability designed for the tactical environment. It provides scalable, enterprise-grade computational power, with pre-engineered secure virtualized infrastructure, essential to AI/ML-driven cognitive weaponizing, enabling real-time analysis of multiple datasets simultaneously. Simultaneous analytics of classified datasets and enabling automation of current air-gap processes offer significant opportunities to accelerate our OODA loop. This NSA-vetted, RTB compliant solution enhances situational awareness and decision-making at the tactical edge, empowering warfighters with actionable intelligence to effectively counter EW threats. Our solution meets the critical need for a compact, secure, versatile tactical edge processing capability that improves operational effectiveness in the electronic warfare domain, allowing the Army to navigate the dynamic EW landscape with confidence.

**BIO:** Therman Farley has served as Trace Systems' Vice President of the Information Solutions Group (ISG) since January 2018. Therman oversees all aspects of the ISG, including financial management, governance, strategic direction, development of the business strategy, as well as oversight for all information systems, innovation, product development and operations. He is a proven leader with significant experience in strategic planning and leading diverse business development efforts and growth opportunities. He is well-versed in emerging technologies and contract and teaming agreement negotiations.

Prior to joining Trace, Therman served as the network operations manager at SAIC in Stuttgart, Germany, providing managerial, technical, functional, supervisory and operational expertise in support of the DoD's wide area network. He further managed network operations, transport and IP in the Theater Networks Operations Center. Therman has served as the chief of Transmissions Network Services Division for the DoD, where he developed, established and maintained strategic business methodology in support of 40+ DISA Europe programs valued at more than \$300 million. He further acted as the European lead for the agency-wide Global Information Grid (GIG) Service Management effort, a \$4.6 billion program.

Therman has a BS in history from the University of South Carolina–Aiken and served 22 years in the U.S. Army, retiring as a major. He is a highly experienced former Army signal officer, with proven ability to manage geographically disparate teams, programs, costs, schedules, risk, resources, and performance on multi-hundred-million-dollar information technology programs on a global level. Therman's professional certifications include Program Management Professional (PMP) (2005) and Information Technology Infrastructure Library (ITIL) v3 Foundations (2008).

# Identifying Non-CVE Risks Within OT & ICS

**Thomas Pace, Co-Founder & CEO, NetRise** • [thomas.pace@netrise.io](mailto:thomas.pace@netrise.io)

## ABSTRACT

The need to identify pressing, exploitable vulnerabilities beyond CVEs has never been more urgent. NetRise CEO Thomas Pace presents on the disparity between device vulnerabilities and our understanding of risk, focusing on often overlooked non-CVE risks.

Vulnerabilities catch the headlines and rightfully so, but there is a gross misconception that a device with 0 CVEs is risk free. This could not be further from the truth, especially for ICS and OT devices. Non-CVE vulnerability arising from public/private key pairs, authentication accounts, plaintext passwords, cloud API keys and misconfigurations is the rule, not the exception. This discussion will cover the causes and effects of unaddressed risk, as well as steps available for direct mitigation and ongoing management of all vulnerabilities — not just those which are publicly available.

**BIO:** Thomas Pace began his career in the U.S. Marine Corps, serving as an infantryman and intelligence specialist while serving on deployments to Iraq and Afghanistan. Thomas held multiple roles as an incident responder, security implementer and security architect. Thomas worked the Strategic Petroleum Reserve for the Department of Energy, where he focused on security engineering as well as industrial control systems security and gained the initial idea for NetRise after consistently dealing with issues within the ICS environment and lacking visibility. Thomas then worked at Cylance, eventually moving into the position of VP, Global Enterprise Solutions, where he acted as the primary sales and technical overlay for all aspects of the company.

# Setting a Fast Path Toward Cloud Adoption

**Tommy Dammer, Senior Solutions Engineer, VMware** • [tdammer@vmware.com](mailto:tdammer@vmware.com)

## ABSTRACT

Learn about DISA Stratus, the DoD Private Cloud powered by VMware. We provide an overview of the architecture, services, pricing and ordering for this IL2-IL6 accredited cloud solution and discuss how to leverage current investments in VMware and take advantage of a fast path toward cloud adoption.

DISA and VMware have partnered to bring the VMware Multi-Cloud to the DoDIN. Stratus is the DoD private cloud designed to provide optionality to mission partners. Stratus provides a multi-tenant, self-service management capability for compute, storage and network infrastructure. It delivers rapid elasticity, resource pooling, and broad network access through a self-service on-demand web-based portal where Mission Partners can manage their resources as needed.

**BIO:** Tommy Dammer has more than 20 years of experience working within the DoD across multiple IT disciplines. As a senior solutions engineer, Tommy currently supports DISA and Fourth Estate Agencies on the design and implementation of hybrid multi-cloud solutions.

# Project Fort Zero End-to-End Solution

**Will Robinson, Federal DoD Chief Strategist, Dell Technologies •**

will.robinson@dell.com

## ABSTRACT

A fully configured Project Fort Zero end-to-end solution will lower the barrier to zero-trust adoption by helping Army organizations adapt and respond to cybersecurity risks while offering the highest level of protection. The solution will be validated in the next 12 months by the U.S. Department of Defense and is part of a Dell Security portfolio expansion.

Project Fort Zero can serve a variety of use cases, including:

- **On-premise environments:** For organizations where data security and compliance are paramount.
- **Tactical and edge node environments:** Where cybersecurity implementation and compliance is needed in a denied, degraded, intermittent and limited bandwidth (DDIL) environments

**BIO:** Will Robinson is Chief Strategist Department of Defense Dell Technologies Services. He is responsible for engaging with clients on strategy, innovation and transformation. Will provides Dell's DoD Executive/Senior-Level leaders consultative and knowledgeable strategy focused on achieving tangible operational/business outcomes for our customers at enterprise scale. Will is accountable for aligning Dell Technologies portfolio to meet customer requirements on multi-cloud to Edge computing, data protection, AI/ML and Dell's professional services.

Previously, Will has served more than 30 years in the U.S. Army as a senior Army warrant officer. He's served as the Army DCS G6 Chief Technology Officer. Led in all areas of IT and cybersecurity; "go to" technical adviser, aiding in development of strategies, plans, implementation, and decisions, including chief technical advisor on Integrated Tactical and Enterprise Networks. Aptly coordinated and partnered with headquarters staff, Department of Defense (DoD), Program Executive Officers (PEOs), academia, industry and federally funded research and development centers, ensuring Army leadership was aware, understood the impact and application of emerging technologies and its Technology Readiness Levels.

Will also serve as the senior technical adviser within the Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASAALT), keenly advising, assisting and supporting the Deputy for Acquisition and Systems Management (DASM), Principal Military Deputy of the Military Departments (PMILDEP), ASAALT staff, and PEOs with relevant strategic technical and operational expertise that informs acquisition decisions.



# Security-First AI

**Zach Vaughn, Director, Federal Security Engineering, Vectra AI •**

zvaughn@vectra.ai

## ABSTRACT

AI and ML are generating a significant amount of hype and attention. Vectra AI can offer security-first AI and make immediate and meaningful impact and uplevel cyber defenders.

**BIO:** Zachary Vaughn is the Director for Federal Security Engineering at Vectra AI. He has been supporting federal agencies for more than 16 years in areas such as access and identity management, web and application security, virtualization of key infrastructure and network security.

# Operationalizing AI in Cyber: Creating Opportunities for Long-Term Strategic Advantage

**Zach Vaughn, Director, Federal Security Engineering, Vectra AI •**  
zvaughn@vectra.ai

## ABSTRACT

It is hard to find an industry untouched by the transformative power of artificial intelligence (AI) and cybersecurity is no exception to this trend. While early AI adopters have enjoyed material advantages, will those advantages regress to mere competitive parity as operationalized AI becomes table stakes for modern cyber? For some organizations the answer will almost certainly be yes, but it doesn't have to be!

Vectra AI offers leaders with a vested interest in establishing, achieving, maintaining or extending their strategic cyber advantages through AI solutions and details principles and process at the center of this challenge, placed in the context of organizational resources, risks, and above all, mission.

**BIO:** Zachary Vaughn is the Director for Federal Security Engineering at Vectra AI. He has been supporting federal agencies for more than 16 years in areas such as access and identity management, web and application security, virtualization of key infrastructure and network security.



## WHAT IS AFCEA?

AFCEA is a member-based, nonprofit association for professionals that provides highly sought-after thought leadership, engagement and networking opportunities. We focus on cyber, command, control, communications, computers and intelligence to address national and international security challenges.

The association has more than 30,000 individual members, 138 chapters and 1,600 corporate members. For more information, visit [www.afcea.org](http://www.afcea.org)

