

# TechNetCyber

---



**2022 SOLUTIONS SHOWCASE**





# AFCEA TechNet Cyber Solutions Review

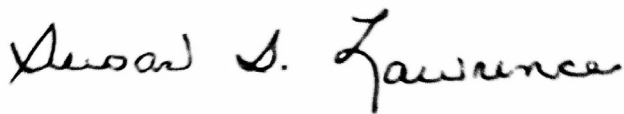
The cyber realm is dynamic and ever-evolving. The nation's competitors grow more sophisticated, more determined and, in some cases, more aggressive day by day.

Just as the technologies, tactics, techniques and procedures in the cyber arena continue to evolve, our training and education efforts must remain agile and adaptable.

The cyber forces are at the forefront of a new kind of competition and conflict, and the role they play is absolutely vital to our national and global security—today and in the future.

TechNet Cyber is designed to open the lines of communication and facilitate networking, education and problem solving. This Solutions Review Compendium complements the event and builds engagement.

Best wishes,

A handwritten signature in black ink that reads "Susan S. Lawrence". The signature is written in a cursive style with a large, prominent 'L' at the end.

**Lt. Gen. Susan S. Lawrence, USA (Ret.)**

President and CEO  
AFCEA International

# Table of Contents

Secure Collaboration in M365 within a Zero Trust Lens John “Jay” Leask, Director of Federal Strategy, AvePoint.....	8
QuARC: Quantum Applications and Resistant Crypto JD Dulny, Director, Strategic Innovation Leader, Booz Allen Hamilton.....	9
Building Toward a Zero-Trust Architecture Michael Lundberg, Principal Solutions Architect, Booz Allen Hamilton .....	10
Analysis of Network KPIs for Intelligent Migration to Edge Compute Marion Tinio, Senior Lead Technologist, Booz Allen Hamilton .....	11
Winning the Edge: Information Superiority through Robust Edge Computing Jose Martinez, Technical Solutions Architect, Cisco.....	12
A Zero-Trust Approach to Implementing Commander’s Intent for Cybersecurity Andrew Stewart, National Security and Government Senior Strategist for Cybersecurity, Cisco .....	14
Myth Busting Zero Trust and Driving toward Mission Assurance Andrew Harris, Sr. Director, Public Sector, Chief Technology Officer, CrowdStrike .....	15
Tensor Computing for Post-Quantum Encryption Jonathan Mullin, Chief Scientist, DCI Solutions .....	16
Cyber Defense from Edge to Enterprise Jonathan Mullin, Chief Scientist, DCI Solutions .....	18

Zero-Trust Networking for Operational Technology	
Wayne Dixon, Senior Solutions Architect, Dragos Federal.....	20
Homomorphic Encryption: A Practitioner’s Guide to Utilizing Breakthroughs in Advanced Cryptography to Meet Mission Needs	
Ryan Carr, Chief Technology Officer and Vice President of Engineering, Enveil.....	21
Zero-Trust Threat Assessments	
Jared Dible, Sr. Technical Account Manager, Millennium Corporation .....	23
Zero Trust 5G Networks: Protecting High-Risk, High-Priority Assets First	
Steve Vogelsang, Chief Technology Officer, Federal Division, Nokia .....	25
Zero-Trust Storage	
Steve Petruzzo, Chief Technology Officer, Qcor .....	26
Scaling Automated Security Validation	
Clint Green, Senior Technical Architect, Rebellion Defense, Inc. ....	27
Accelerate the Mission with Zero Trust Secure AI Access to the Edge	
Andrew Whelchel, Senior Solutions Engineer – Federal, Saviynt.....	29
Making Zero Trust Work for You	
Kevin Brooks, Principal Digital Strategist, ServiceNow.....	30
Quantum-Resistant Security	
Bill Becker, Chief Technology Officer, Thales TCT .....	32

# Table of Contents

Zero Trust: Beyond the Buzzword Bill Becker, Chief Technology Officer, Thales TCT .....	33
Security From Compliance within a Zero-Trust Architecture Keith Driver, Chief Technology Officer, Titania Ltd. ....	34
RPA in the SOC: Human-Machine Teaming for Threat Response Bill Nystrom, Defense Cyberspace and IT Automation Leader and Strategist, UiPath .....	35
Cybersecurity in the Age of Zero Trust Mike Malaret, Technical Director, U.S. Public Sector, Veritas Technologies .....	36
Zero-Trust Architecture for Mission-Critical Operations: From Sensor and Cloud to Tactical Edge Nicholas Lessen, Solutions Architect, Forcepoint .....	37
A New Approach to Modernize Your Zero-Trust Architecture Steve Ryan, Founder and CEO, Trinity Cyber Inc .....	38
Cyber Forza Zero-Trust Compliant Architecture Implementation and Case Study Dr. Venkat Rayapati, Founder and CEO, Cyber Forza, Inc. ....	40
Aligning ICAM, the Executive Order & Zero Trust for the Defense Department Josh Brodbent, RVP Public Sector Solutions Engineering, BeyondTrust.....	42
RMF Acceleration through eMASS Automation Brian Hajost, Founder and Chief Operating Officer, SteelCloud .....	43

Extensible Zero-Trust Framework at the Digital Edge	
Don Wiggins, Global Chief Solutions Architect, Equinix.....	44
Future of the Edge: Overmatch for Secure Edge Platforms	
Brad Sollar, Chief Technology Officer, Mainsail Industries.....	46
Deploying Multi-Mission Workloads at Scale	
Jason Strawderman, Senior Director of Sales and Business Development, Facility Security Officer and Co-Founder, Western Digital Federal .....	48
Distributed Zero-Trust Security	
Kim Van Der Wende, Field & Channel Marketing Manager – Federal, Palo Alto Networks.....	49
Zero Trust Hardware Access	
Yossi Appleboum, CEO, Sepio .....	50
DOD Edge 2.0	
Michael Rau, Senior Vice President of Solutions Engineering and Enablement, F5 .....	51

# Secure Collaboration in M365 within a Zero Trust Lens

**John “Jay” Leask, Director of Federal Strategy, AvePoint • jay.leask@avepoint.com**

## ABSTRACT

Microsoft 365 quickly brings together collaborators across your agency and your partners. That built-in collaboration, however, creates new concerns around tracking who has access across your environment. Organizations must monitor how users interact with data within a zero-trust architecture.

When viewed individually, core pillars of zero trust, such as network, data and user, are bound in M365:

- How is our service secured?
- How do we protect sensitive data?
- Which users do we authenticate in our system?

However, this approach misses the intersection across zero-trust pillars in the collaboration spaces themselves. This solutions statement addresses how defense agencies can leverage Microsoft 365's collaborative power while including a zero-trust model.

We discuss:

- Automating policy enforcement at the workspace (Teams, SharePoint and M365 Groups)
- Workspace compliance, lifecycle and permissions recertification based on data sensitivity
- Intelligent reporting of exposure risk based on sensitive information types and permissions data

**BIO:** John “Jay” Leask is the director of Federal Strategy at AvePoint.



# QuARC: Quantum Applications and Resistant Crypto

**JD Dulny, Director, Strategic Innovation Leader, Booz Allen Hamilton •**

dulny\_jd@bah.com

## ABSTRACT

Emerging quantum technologies will have a transformational effect across the government. Continued progress in quantum computing foreshadows a disruptive cryptographic transition due to known quantum algorithms capable of breaking widely deployed public-key cryptography.

The services and capabilities used throughout the government to authenticate users, protect the confidentiality of classified materials and verify the integrity of information are at risk. As a proven performer in the quantum and cybersecurity space for the government, Booz Allen recognizes the operational complexity around adopting new cryptographic standards.

In this solutions statement, we take a broad survey of the services, requirements and capabilities designed to mitigate this coming threat. We demonstrate quantum-safe applications to illustrate how post-quantum cryptography algorithms can be tested today.

To prepare for the coming transition, we outline the journey complex organizations must begin to undertake to fully realize a quantum-safe posture across their security enterprise.

**BIO:** JD Dulny is a strategic innovation leader at Booz Allen. A Ph.D. physicist, JD serves as the firmwide lead for quantum information sciences and as an executive leader within the firm's artificial intelligence business. JD and the quantum team study cutting-edge quantum computing, communication and sensing technologies. The quantum team puts these critical new technologies in the context of our clients' missions, providing insight into how they can be applied to address frontier problems in optimization, machine learning, information security and beyond. The team has become one of the largest groups in the field worldwide, contributing to the scientific community by authoring key publications while also providing thought leadership for client missions. JD earned his Ph.D. in computational physics from Penn State University, where he focused on large-scale Monte Carlo studies of complex surface phenomena.

He holds a B.S. in physics from the University of Maryland, Baltimore County.

# Building Toward a Zero-Trust Architecture

**Michael Lundberg, Principal Solutions Architect, Booz Allen Hamilton •**

lundberg\_michael@bah.com

## ABSTRACT

Threat actors continue to bypass traditional perimeter security defenses, prompting organizations to shift to a zero-trust (ZT) mindset where cybersecurity designs focus on protecting an organization's data and access to that data versus relying on protecting the network from a breach. This data centric cybersecurity approach requires developing a comprehensive data tagging and labeling strategy where the criticality of an organization's data is fully understood, allowing for policy rules and enforcement to occur as users and systems try to access that data.

Two key factors should be used to determine user or system access to that data, including identifying the user/system via an identity, credential and access management (ICAM) solution and examining the device's posture (e.g., antivirus status, patching status encryption status). The combination of the identity and device posture allows for granular decision-making and policy enforcement for accessing data.

Modernization of visibility and analytics for an organization's on-premises, hybrid, and/or multi-cloud environment and its remote workforce is just as important as the implementation of conditional based access to data and workloads. To keep pace with advancing threats and distributed users and workloads, organizations need a distributed data analytics architecture to process logs as close as possible to the source, while centralizing visibility of relevant events and alerts to analysts and operators. Booz Allen is helping the Defense Department, intelligence community, civil and commercial organizations modernize their current brownfield environments to incrementally move toward a zero-trust architecture, including assessing their current ZT maturity, identifying gaps, developing roadmaps and implementing new solutions.

This presentation outlines how organizations can incrementally move toward a ZTA by:

1. Moving away from traditional VPN architectures to Secure Access Service Edge (SASE) solutions to enforce conditional-based access for remote users, while optimizing performance (i.e., direct to cloud)
2. Moving away from traditional centralized security stacks to a software defined wide area network (SD-WAN) and customer edge security stacks (CESS) to simplify management, improve performance and apply conditional-based access and micro-segmentation at the application layer for on-premises users
3. Moving away from centralized data lakes and analytics to distributed data analytics to optimize detection, reduce costs and improve the information provided to defense cyber operations (DCO) analysts in a hybrid, multi-cloud environment.

**BIO:** Michael Lundberg is a Principal Solutions Architect at Booz Allen, where he leads the firm's ZT strategic investments and multiple ZT engagements across commercial, federal and Defense Department organizations, including ZT assessments, architectures and implementations. Michael has more than 16 years of experience designing and architecting networking and cybersecurity solutions for the Defense Information Systems Agency (DISA) and the DoD. He is the integrator lead solutions architect of DISA's Thunderdome ZT implementation.

# Analysis of Network KPIs for Intelligent Migration to Edge Compute

**Marion Tinio, Senior Lead Technologist, Booz Allen Hamilton •**

tinio\_marion@bah.com

## ABSTRACT

The Department of Defense (DoD) has been engaged in a multi-year cloud-first strategy and has been steadily migrating applications and services to public and private clouds. These cloud environments offer ubiquitous, inexpensive and scalable compute—but with geo-political challenges and the need to support mission critical operations globally, a solution to intelligently move applications and data between regional clouds and to the tactical edge is required to ensure access applications and data at the point of need.

Network quality and the capability to reach back to enterprise clouds degrades rapidly as forces deploy, and at a certain point it is necessary to move the application and data to the edge. Understanding that point requires real-time analysis of multiple data points including latency, jitter, packet loss and uptime—and the ability to coordinate the movement of processing to the edge.

We present a reference architecture and model for service providers and cloud consumers to adopt that enables migration of workloads between edge and enterprise cloud platforms. Real-time analysis of metrics and Key Performance Indicators (KPIs) must inform these advanced models for seamlessly making intelligent decisions. We also discuss recommended follow-on research to consider other factors that weigh on an agency's decisions for edge processing, including local power grid utilization, carbon footprint, geopolitical tensions and cost.

Furthermore, local challenges could necessitate the use of remote enterprise cloud capabilities despite the lower network quality, including a power outage, technical glitch or regional disaster. These complex scenarios and decisions necessitate incorporating artificial intelligence (AI) models and digital twin technologies to make decisions that optimize the underlying hybrid-, multi- and edge-cloud infrastructure.

**BIO:** Marion Tinio is a leader in Booz Allen's Strategic Innovation Group. She is a cloud security architect serving as the chief architect for a large government organization's Amazon Web Services FedRAMP accredited platform, as well as leading the firmwide Edge Cloud capability investments.

With Marion's experience supporting workloads in the cloud, she has insight into common pain points and challenges with the adoption of the current cloud delivery model. Marion leads the Edge Cloud investment team in research and prototyping emerging technologies to deliver faster processing time, improved redundancy and reduced latency for better user experience.

As edge cloud relies on multiple areas of IT, the team provides insight into best of breed technologies across networking, computing, automation and microservices and how to integrate them to meet our clients' missions.

Marion holds a B.S. in electrical engineering from the Georgia Institute of Technology.

# Winning the Edge: Information Superiority through Robust Edge Computing

**Jose Martinez, Technical Solutions Architect, Cisco** • jomartin@cisco.com

## ABSTRACT

Battles are fought and won at the edge. Whether supporting the mission or executing it, modern operations require distributed technologies with enterprise capability. Delivering to the edge takes secure, integrated and open solutions across hybrid clouds through the WAN at the speed and scale of warfare.

According to Gartner, “around 10% of enterprise-generated data is created and processed outside a traditional centralized data center or cloud. By 2025, Gartner predicts this figure will reach 75%.”

The Edge Computing framework allows organizations to shift computing resources for their applications from central data centers, private clouds or public clouds to locations closer to the endpoints and end-users that need it most. In practical terms, this means enterprise computing at the tactical edge delivered via a robust, flexible, easy to scale and secure infrastructure.

Cisco’s end-to-end data center solution extends from on-prem to private and public clouds all the way to the edge. Cisco Hyperflex is a hyperconverged infrastructure (HCI) solution built for the edge with two, three or four nodes per cluster and incorporates powerful data optimization features. Clusters are deployed rapidly anywhere on the globe with no on-site expertise via a powerful operations platform directly from the Defense Information Systems Agency (DISA) cloud.

The Cisco Intersight platform delivers intelligent visualization, optimization and orchestration for applications and infrastructure across the entire hybrid environment. HCI is one component required to deliver applications across edge, data center and cloud. A proper software-defined network (SDN) solution is the other. Cisco again delivers with two SDN technology leaders.

Since its development in 2012, Cisco ACI has been the industry’s most secure, open and comprehensive SDN data center solution. ACI enables automation accelerating infrastructure deployment and governance, simplifying workload mobility across a multi-fabric, hybrid cloud or multi-cloud framework, and proactively secures against risk arising from anywhere. Cisco ACI enables customers to build a truly agile and resilient data center with policies that can move anywhere through automation.

Global transport requires WAN solutions. The ACI data center solution integrates with Cisco SD-WAN for comprehensive software defined networking. Cisco SD-WAN is a highly secure, cloud-scale architecture that is open, programmable and scalable. SD-WAN connects data centers, branches, campuses and colocation facilities to improve network speed, security and efficiency. All these solutions provide a northbound API access enabling orchestration to automatically modify the environment and adjust to changes in requirements.

Creating a bridge between intent and action requires an orchestrator that supports multiple vendors. The Cisco Network Service Orchestrator (NSO) provides a robust bridge linking network automation and orchestration tools with the underlying physical and virtual infrastructure. Its rich set of software interfaces and APIs allows straightforward northbound integration. An extensible southbound device abstraction layer means NSO works with multiple vendors and multiple technology domains. Cisco's Edge Computing solution is the comprehensive standard, meeting the most critical demands of the DoD and delivering information at the speed of warfare.

**BIO:** Jose Martinez is a Data Center Technical Solution Architect supporting U.S. federal customers. He has more than 20 years of experience supporting customers in both pre- & post-sales environments. Jose joined Cisco System in 1995 and has worked in multiple teams supporting different technologies, including L2 & L3 switches, voice gateways, Unified Communications (CallManager) and most recently Data Center technologies.

He has been a presenter at Cisco Live events in the United States, Europe and Australia and has traveled around the United States and Europe providing tech talks at partners and user-groups events.

# A Zero-Trust Approach to Implementing Commander's Intent for Cybersecurity

**Andrew Stewart, National Security and Government Senior Strategist for Cybersecurity, Cisco • [andrewst@cisco.com](mailto:andrewst@cisco.com)**

## ABSTRACT

A zero-trust design strategy based on a platform-approach that constantly enforces least-privilege access from edge to hybrid multi-cloud is the operational outcome for a software-defined network that satisfies Commander's Intent for Cybersecurity and Department of Defense Network Operations.

Implementing the Commander's Intent for Cybersecurity means applying, monitoring and enforcing network controls as operational policies, including DoD Comply-to-Connect (C2C) requirements and integrating all network controlling actions across the enterprise—from users/endpoints to data and applications—no matter where they reside. By implementing Commander's Intent for Cybersecurity, operations on DoD networks can be transformed into a real-time, network operational platform capability. Just like Commander's intent is applied through controlling actions and maneuver orders to units of action (according to the unit's identity and defined capabilities), so too must effective cybersecurity policy (Commander's Intent) be applied to users, devices and applications with knowledge of their status, how they are connected to the network, their allowed data, applications and functions on the network—with verification and validation—continuously, at speed and scale.

Operationalizing the DoD Network Platform with this zero-trust design approach will satisfy Commander's Intent for Cybersecurity.

**BIO:** Capt. Andrew D. Stewart, USN (Ret.) is a National Security and Government Senior Strategist for Cybersecurity at Cisco Systems, Inc. He works across Cisco's Global Government practice, focusing primarily on national defense and intelligence. He has been with Cisco since 2019 after retiring from almost 30 years in the U.S. Navy, where he last served as the chief of cyber operations for the Fleet Cyber Command/U.S. TENTH Fleet.

Andy also served as the Commanding Officer and Program Manager for Navy Cyber Warfare Development Group (NCWDG)/Commander, Task Force 1090, responsible for the Navy's Cyber Warfare operations and innovation enterprise for rapid capabilities development and ACAT-II program of record. During his tenure, NCWDG received the 2016 National Security Agency Director's Trophy. He is a graduate of the Sellinger School of Business and Management, Loyola University in Maryland and the Cybersecurity and Policy Executive Program from the Harvard Kennedy School. He is also a graduate of the Naval Postgraduate School Monterey, California, the U.S. Naval Academy, the National Defense University and the Naval War College. He is a recipient of the National Defense University Foundation Award and the 2003 AFCEA Copernicus Award.

# Myth Busting Zero Trust and Driving toward Mission Assurance

**Andrew Harris, Sr. Director, Public Sector, Chief Technology Officer, CrowdStrike**

• [andrew.harris@crowdstrike.com](mailto:andrew.harris@crowdstrike.com)

## ABSTRACT

Zero trust has become a marketing term, causing confusion and negative impact toward mission resilience. In this solutions document, CrowdStrike discusses how the company has helped the Department of Homeland Security, Fortune 500 firms and entities within the financial sector move toward their paths of zero trust—focusing on the outcome and starting where the customer is, today.

We use the SolarWinds breach as an example, illustrating the multiple enforcement and decision points in the architecture, and what customers should expect from their vendors in the future in the spirit of zero trust—and more importantly, enhancing mission resilience.

**BIO:** Andrew Harris has 15+ years of experience in cybersecurity, most of which has been in supporting or leading some of the most sensitive U.S. government agencies. Andrew is CrowdStrike's Sr. Director for Public Sector Technology Strategy, where he is responsible for driving innovation and ensuring technical alignment across product groups and with public sector customers. Prior to joining CrowdStrike, Andrew worked at Microsoft as a Principal Program Manager, where he focused on engineering solutions across 50+ products while focusing on more than \$1 billion major government contracts. He served as the chief technology officer for the Customer Experience Engineering (CxE) team for Azure Security, where he also drove product strategy. Andrew led the Recovery team at Microsoft for Incident Response and helped the National Institute of Standards and Technology (NIST) write the playbook on SP 800-184, "Guide for Cybersecurity Event Recovery." Andrew also served as a special adviser to the White House, U.S. House of Representatives, multiple military services within the Department of Defense, New York City Police Department and various Fortune 100 companies. Prior to Microsoft, Andrew was the chief of strategic programs at the Defense Information Systems Agency (DISA), pioneering Department of Defense Enterprise cybersecurity programs, most of which are fully deployed and remain top priorities for the Pentagon.

# Tensor Computing for Post-Quantum Encryption

**Jonathan Mullin, Chief Scientist, DCI Solutions** • [jmullin@dcj-solutions.com](mailto:jmullin@dcj-solutions.com)

## ABSTRACT

To achieve highest efficiency for computation specialized hardware, namely Fixed Programmable Gate Arrays (FPGA) or Application-Specific Integrated Circuits (ASICs) are used to reduce the SWAP of a system. While this hardware has been effective, the consumer market products have encroached on their performance per watt with the rise of high-performance Single Instruction Multiple Data (SIMD) architectures. This coupled with the ease of programming SIMD architectures make them a viable platform for development of a new low SWAP encryption platforms. Additionally, recent advances in tensor-based error correcting algorithms have pushed the boundary of compute per watt.

These advances allow for a tuning of hardware and software meeting the forthcoming National Institute of Standards and Technology-approved quantum resistant algorithms. Our interest lies with the learning with errors (LWE) algorithms. LWE-based schemes are appealing in theory and for practical reasons. On the theoretical side, LWE-based schemes offer a strong security guarantee. The LWE problem is equivalent to the problem of decoding random linear codes, a problem that has been extensively studied in the last 50 years. The fastest known algorithms run in exponential time, and unlike most number-theoretic problems used in cryptography, the LWE problem does not succumb to known quantum algorithms.

On the practical side, LWE-based schemes are often extremely simple and efficient in terms of code-size and time and memory requirements. This makes them prime candidates for light-weight/low power devices such as RFID tags, which are too weak to implement standard cryptographic primitives such as the AES block-cipher. This proven ability in low power systems makes LWE an excellent candidate for low SWAP-embedded encryption devices. With the hardware advances, these algorithms are well suited to use the latest C-based compilers for SIMD architecture optimization.

Our initial test bed will most likely be an NVIDIA system, however the offerings from AMD and Intel are compelling options. One benefit of the SIMD architecture is the rapid development of the competing platforms. With the current race for high-end HPC dominance in the exascale computing initiatives, the efficiency of these chips is constantly improving. As lower-end models become available in the following years, they benefit from the enormous R&D efforts yielding remarkably efficient embedded devices. An example is the model board we initially have been using and which is based on a 6-year-old architecture; slightly larger models using the latest architecture have 4 times the improvement on performance/Watt.

We are just starting to explore the use of tensor cores for this area after recent advances yielding double the throughput of matrix-matrix multiplications at half the watt/s. By focusing on power efficiency and tunable error tolerance allowed by the LWE approach, we believe this coupling of hardware and software can yield efficient post quantum cryptographic devices on commodity hardware. NVIDIA has taken the lead in the embedded space thus far and has had several platforms hardened for use in currently deployed DoD systems.



**BIO:** Jonathan Mullin is the chief scientist at DCI Solutions. He has more than 20 years of experience identifying and delivering solutions for the Defense Department's most challenging problems in machine learning, high performance computing, quantum and material sciences, data science and cybersecurity, using HPC and artificial intelligence/machine learning to push what is possible and meet the government's unique unclassified and classified challenges. He has more than 10 years of experience leading teams to deliver bespoke data analysis tools for a variety of unstructured and structured data sets. His work has focused on technical leadership and management of programs at academic institutions, startup companies, research laboratories for the U.S. Air Force Research, Army and Navy, and the Army C5ISR center of excellence.

# Cyber Defense from Edge to Enterprise

**Jonathan Mullin, Chief Scientist, DCI Solutions • [jmullin@dcj-solutions.com](mailto:jmullin@dcj-solutions.com)**

## ABSTRACT

TriNNity harnesses the power of machine learning (ML) for the purpose of anomaly detection. TriNNity is powered by state-of-the-art transformer models to defend against never-before-seen cyberattacks at the network and host level. Transformer models have dramatically increased computers' ability to respond to human language input in tasks, including web searches, language translation, chat bots and generating prose.

DCI Solutions is a pioneer in bringing transformer models to the cyber domain for anomaly detection using TriNNity. TriNNity is not another fine-tuned BERT model, but takes the approach of training light, efficient models from scratch using cyber data. TriNNity repurposes the cross-entropy loss function typically used to train a transformer model to the task of anomaly detection. Unlike supervised methods, TriNNity's self-supervised method generates internal labels from the structure of the data. This is a big deal because it is impractical to try to label the large volumes of cyber data generated by even small networks. Self-supervised learning also has the very important benefit of detecting never-before-seen threats. Self-supervision is sort of like a clustering method on steroids because it can take advantage of the structure of the data to generate internal labels.

A recent study conducted by DCI employees found TriNNity to have 0.98 precision, 1.00 Recall and an F1 score of 0.99. During the study, an eternal blue exploit was carried out on a medium-sized enterprise network emulated by CyberVAN. TriNNity was able detect every host that was infected by eternal blue, with very few false positives. The false positives noted were associated with non-malicious, anomalous events such as a kernel panic. Not only was TriNNity's detection performance near perfect, it was also very fast, with most infections detected within one minute. The transformer model that forms the basis of TriNNity also lends itself nicely to interpretation. The model uses attention weights to determine anomaly scores that can give a cyberhunter direct insight into what the model is paying attention to when it detects anomalous events. After proving out the concept of TriNNity, DCI Solutions teamed up with NVIDIA to use NVIDIA's Morpheus framework to bring TriNNity to production at scale from handheld devices to multiple servers. Morpheus uses a collection of solutions contained within kubernetes/docker containers to bring cyber ML solutions to traditional servers along with more modern cloud/VM based networks.

The ELK stack delivers scalability, replication and high throughput of cyber data. RAPIDS puts data preprocessing onto GPUs increasing processing speeds by 66 times and tokenization by 650 times.

TensorRT optimizes models for a given GPU, which we found to give a 4.2 times boost. Triton keeps everything in GPU memory across multiple GPUs across multiples servers. Triton enables dynamic batching to meet the latency requirements of the network. By optimizing TriNNity for GPUs, Morpheus enables a production-level cyber ML pipeline suited for any network environment. DCI Solutions is recently revealed TriNNity and its recent successes with NVIDIA's Morpheus at this year's GTC conference in March.

**BIO:** Jonathan Mullin is the chief scientist at DCI Solutions. He has more than 20 years of experience identifying and delivering solutions for the Defense Department's most challenging problems in machine learning, high performance computing, quantum and material sciences, data science and cybersecurity, using HPC and artificial intelligence/machine learning to push what is possible and meet the government's unique unclassified and classified challenges. He has more than 10 years of experience leading teams to deliver bespoke data analysis tools for a variety of unstructured and structured data sets. His work has focused on technical leadership and management of programs at academic institutions, startup companies, research laboratories for the U.S. Air Force Research, Army and Navy, and the Army C5ISR center of excellence.

# Zero-Trust Networking for Operational Technology

**Wayne Dixon, Senior Solutions Architect, Dragos Federal •**

adowney@dragos.com

## ABSTRACT

The issue of Cybersecurity for Operational Technology has been steadily increasing year over year. While industrial digitalization has brought many efficiencies to our processes, it has also left critical assets more vulnerable than ever before. Evidence of this can be seen in several high-profile incidents, leading the White House to update Executive Order 13920, specifically calling out cybersecurity as a key focus area for the nation's bulk power assets.

As many traditional cybersecurity controls are not well suited for operational technology (OT), asset owners are looking for mechanisms to improve their asset's resiliency to cybersecurity incidents in ways that minimizes impact to their asset's mission.

This is where zero-trust networking is proving to be a compelling option, allowing asset owners to prioritize vulnerability mitigation vs the traditional approach of vulnerability remediation. In this solutions statement we explore what it is about zero-trust networking that makes it such a compelling option for OT.

Topics include:

- Zero-trust networking concepts
- The Benefits of zero-trust networking for OT assets
- Getting started with a zero-trust networking project in OT
- Deploying and maturing zero-trust networking in OT

**BIO:** Wayne Dixon, Senior Solutions Architect for Dragos Federal, has more than 20 years of experience in information technology and has been specifically focused on industrial control solutions/operation technology (OT) cybersecurity for the past decade. Previously the Director of OT and Industrial Solutions at Forescout Technologies, Inc., Wayne comes to Dragos as a subject matter expert with a strong passion for protecting civilization by preventing and identifying cyber threats through assessments and incident response observations.

# Homomorphic Encryption: A Practitioner's Guide to Utilizing Breakthroughs in Advanced Cryptography to Meet Mission Needs

**Ryan Carr, Chief Technology Officer and Vice President of Engineering, Enveil •**

[lisa@enveil.com](mailto:lisa@enveil.com)

## ABSTRACT

Recent advances in homomorphic encryption (HE), a pillar of the increasingly important technology category known as privacy enhancing technologies (PETs), are changing the paradigm of secure data usage for mission use cases. HE protects data while it's being used or processed by allowing computations to occur in the encrypted or ciphertext domain, and most of the primitives that are currently used for HE are resistant to hypothesized quantum computing attacks.

These powerful capabilities have led to HE being referred to as the “holy grail” of cryptography and are why it has been the subject of research and academic pursuit for nearly four decades.

Once computationally impractical for use at scale, recent performance and utilization breakthroughs are redefining how and where organizations can leverage data to unlock value. HE is transformative because the mission-enabling capabilities it delivers are not making something better; they are making something entirely new possible.

By enabling users to encrypt the content of their search, analytic or machine learning model as well as the associated results, organizations can securely leverage publicly available, open-source, and/or low-side, government-curated data sources while protecting their interests and intent. DOD users can perform secure searches, watch-listing, and analytics using sensitive/classified indicators against publicly available information (PAI) or other less sensitive data on untrusted systems without moving/replicating data or compromising mission objectives. HE significantly expands the way in which external and lower-trust data sources can be effectively leveraged and is serving as an important component of a zero-trust architecture.

These capabilities have far-reaching implications across the USG mission space in applications including high-to-high and high-to-low secure search and tactical edge use cases. In this solutions statement, we will:

- Provide a brief history of homomorphic encryption and the attributes that make the technology stand out.
- Demystify the HE market landscape, highlighting the distinctions between HE researchers, libraries, and solution providers.

- Outline the security and intelligence challenges HE is uniquely positioned to overcome, and how those capabilities can significantly reduce operational risk and accelerate the timeline for turning raw data into actionable intelligence.
- Discuss how HE can power mission-enabling capabilities for the future, including the technology's role in a zero-trust architecture.

**BIO:** Ryan Carr serves as chief technology officer and vice president of engineering at Enveil, the pioneering privacy enhancing technology company protecting data in use. With experience in leading engineering efforts at institutions such as the Johns Hopkins University Applied Physics Laboratory, Ryan's fields of expertise include large-scale analytic systems, distributed algorithms, artificial intelligence, game theory and social learning, and applying cloud computing techniques to simulate and analyze complex interactions among large numbers of autonomous agents.

His research in these areas has been published in highly competitive venues such as Proceedings of the Royal Society, AAI and AAMAS.

Ryan holds a Ph.D. and B.S. in computer science.

# Zero-Trust Threat Assessments

**Jared Dible, Sr. Technical Account Manager, Millennium Corporation •**  
jared.dible@millgroupinc.com

## ABSTRACT

“Zero Trust But Verify Zero Trust” is a drastic shift in securing the DOD’s information systems. For too long, adversaries have been able to compromise the “hard shell” of the DOD’s perimeter and move unabated throughout the department’s many complex networks. While zero trust offers an effective model for authentication and authorization of all activities in an environment, implementation of such a model presents significant challenges. The greatest of these, is answering the question “are we truly better protected?”

While zero-trust guidance and reference architectures exist to aid cybersecurity professionals, software developers and IT practitioners in the implementation of zero trust, there is no standard model and approach to validate whether zero trust is effective. This presents a significant risk in terms of heavy effort committed by resources throughout the DOD to implement solutions that are discovered, through real-world compromises, to be no more effective than the existing perimeter defense model. Validation of zero-trust architectures and implementations is a task that requires a significant familiarity with adversarial tactics, techniques and procedures, combined with a tailored approach to assessing zero-trust deployments.

Such a validation model must be capable of delivering actionable and prioritized results that have immediate and long-term impacts on the security posture of the implemented system. This model should align and support the defined implementation phases in the DOD zero-trust reference architecture. Millennium Corporation has developed the Threat Informed Mission Risk (TIMR) assessment model to evaluate zero-trust implementations effectively and efficiently from the adversarial perspective. Determining the value of zero-trust implementations cannot be accomplished on paper, but must be demonstrated through representative threat assessments, designed to test the environment in the same realistic conditions that are expected during operation. TIMR is a robust and tailored process that provides actionable insight to mission risk for Millennium customers. This process implements a progressive approach to comprehensive security assessments allowing the phases to build on each other without the need to accomplish previous steps. The TIMR model is accomplished in six phases shown below. Once a cycle is completed, those results are pushed back into the next assessment.

This creates a continuous model that compounds on itself and continues to provide strategic and operational value.

1. Assessment development
2. Vulnerability and penetration testing
3. Cyber intelligence
4. Cyber table-top exercise (C-TTX)
5. Adversarial assessment

Along with the six phases of TIMR, the model is supported with continuous mitigation support and software and tool development. Continuous mitigation support delivers real-time actionable strategies to mitigate threats in a prioritized manner based on a mission risk. The continuous support of software and tool development facilitates true adversarial replication and the ability to overcome challenging technical situations to maximize the impact of the assessment model. The TIMR assessment model will validate and secure any zero-trust implementation or technology. It is not enough to just implement zero trust—as the Russian proverb says: you must Trust, but Verify.

**BIO:** Jared Dible has a wide range of technical expertise between cyber operations and systems engineering supporting all branches of the U.S. Defense Department. Jared started his career as a cryptologic technician with the U.S. Navy, where he supported various Signals Intelligence systems until his departure from the Navy as a petty officer 1st class. Afterwards, Jared became an integral part of the DCGS-AF community as a system engineer supporting the U2 Primary Mission Equipment and conducting high-altitude missions across the globe. Following DCGS-AF, Jared became a technical lead on one of the 11 National Security Agency certified and U.S. Cyber Command accredited red teams, where he led more than 35 red team assessments against DOD networks and weapon systems. Prior to joining Millennium as a senior technical account manager, Jared was an Army civilian supporting OSD DOT&E Cybersecurity Assessment Program (CAP), where he planned and executed assessments against combatant commands and their subordinate commands.



# Zero Trust 5G Networks: Protecting High-Risk, High-Priority Assets First

**Steve Vogelsang, Chief Technology Officer, Federal Division, Nokia •**

jacqueline.lampert@nokia.com

## ABSTRACT

Cyber threats are on the rise, becoming more sophisticated and exacerbated by user mobility and proliferation of Internet of Things (IoT) devices connected to the network. The prevalence of malicious activity, such as phishing and ransomware, put federal networks at risk. Network resources must ensure that users or applications are properly and sufficiently authenticated before access is granted. Nokia's capabilities provide a stronger security posture in a zero-trust environment that helps the federal government dramatically reduce the risk of successful cyberattacks against its digital infrastructure by layering security into the network. As a leader in both 5G and IP/optical transport technology, Nokia has developed a zero-trust security architecture that embeds security into the 5G core, transport and IP/optical networks. This includes multiple layers of encryption that significantly increase the security posture of government networks when operating on dedicated infrastructure or through trusted or untrusted networks.

**BIO:** Steve Vogelsang is the chief technology officer (CTO) for Nokia's Federal Division. As CTO, Steve is responsible for leading a technical team that curates and adapts Nokia's broad portfolio of networking products and technology to deliver mission-critical capabilities to the U.S. government. He joined the company through the acquisition of Alcatel-Lucent and brings more than 30 years of technology experience in IP and optical networks. Most recently, Steve was the vice president of strategy and technology for Nokia's Network Infrastructure division, where he helped launch new technology offerings, including IP network analytics and security, data center switching, client optics, optics integration with ASICs and Silicon photonics. Steve holds a Bachelor of Science degree in computer engineering from Carnegie Mellon University. He also holds two patents in state-efficient network function support and ATM communications system, UBR-ABR gateway.

# Zero-Trust Storage

**Steve Petruzzo, Chief Technology Officer, Qcor • [steve.petruzzo@qcor.com](mailto:steve.petruzzo@qcor.com)**

## ABSTRACT

Encryption alone is not the answer to stop ransomware, viruses and other destructive events. It is a common misunderstanding that by using encryption that data is secure. Encrypted data can still be deleted, or re-encrypted by ransomware, which denies access to your data. Data confidentiality is only half of the security equation. Encryption is used to prevent data loss in the form of exfiltration, disclosure or the ability of an adversary to use or exploit your sensitive data for their gain or profit, or for your embarrassment. Data integrity is the missing half of the equation to prevent data alteration, deletion, sabotage, modification, virus injection or ransomware. This is commonly NOT solved by conventional security products because the immutable technology required to prevent alteration and deletion is newly available from Qcor. ForceField is a new technology with enforcement at the lowest layer in the security stack, within each hardware device. ForceField automatically and continuously implements block-level protection with four Policy Enforcement Points of Zero-Trust Architecture, including enforcement at the lowest layer within the hardware itself, and cannot be bypassed regardless of permissions, OS or computer systems used. These technologies are the secure storage used by four National Institute of Standards and Technology best practice projects for data integrity, data confidentiality and protection from ransomware and other destructive events. Data on individual devices, SAN/NAS and in the cloud remains online and protected from ransomware and other cyberattacks with seamless integration of applications with AWS, Google, Azure or other cloud providers.

**BIO:** For more than 35 years, Steve Petruzzo has designed cybersecurity systems and patented secure storage technologies for the federal government and private corporations. These patented immutable zero-trust storage products are used by four National Institute of Standards and Technology best practice projects for data integrity, data confidentiality and prevention of ransomware and other destructive events to prevent data sabotage, viruses, manipulation and deletion.

# Scaling Automated Security Validation

**Clint Green, Senior Technical Architect, Rebellion Defense, Inc. •**

wendy@rebelliondefense.com

## ABSTRACT

The Defense Department's primary means to mitigate cyber risks by having highly trained red teams paid to probe friendly networks to identify and mitigate vulnerabilities before they can be exploited by adversaries is not scalable. A high-demand/low-density asset, DOD red teams remain out of reach for most DOD entities. Although manual red team operations can effectively test network defenses; annual or biannual red team operations cannot keep pace with adversaries who are constantly changing tactics, techniques and procedures (TTPs). To harden defenses, blue teams need more and better opportunities to learn, practice and test their methods before adversaries launch attacks, not just once a year in a simulated, coordinated exercise, but continuously, moving at the pace of adversaries. Rebellion addresses this need by serving as the blue team's on-demand adversary. We arm DOD cyber defenders with continuous, automated, penetration testing and red team operations capability via our Nova cyber readiness software.

Unlike manual security operations, passive scans or other common tools, Rebellion Nova provides ongoing network and system testing using the same TTPs as actual threat actors. In doing so, Nova enables DOD system defenders to test their defenses on demand, mitigating the need to wait months for a human team to become available. Nova gives blue teams realistic, automated adversaries against which to measure their efforts before facing actual adversaries in a real-world attack. Over time, defenders can track their overall cyber posture, assessing the effectiveness of their efforts as personnel change, as training is completed, and as adversaries evolve their methods. Users can validate cyber readiness continuously and keep pace with the dynamic threat landscape with Nova. Nova affords cybersecurity defenders the ability to continuously and proactively probe their defenses based on the perspective and methods of actual adversaries. Furthermore, as system and network configurations evolve over time, defenders can automatically retest defenses against the latest adversarial techniques. Nova also performs continuous reconnaissance of a system, mapping its components, cataloging its assets, and probing for known vulnerabilities and weaknesses. Nova's features test the outcomes of the cybersecurity program, taking into account adversaries' choices among varied attack methods, and the types of attacks they might launch against a system. Nova automates the adversarial testing processes while complementing and augmenting human operators' skill sets. Built exclusively to meet military needs, Nova strengthens the cybersecurity posture and configuration of DOD systems and networks and provides enhanced situational awareness network defenders require to support and deliver positive mission outcomes. Nova is purpose built to integrate easily with existing security software to complement and maximize the value of the DOD's cybersecurity investments. Network operators are empowered to flag network assets as critical, prioritize remediation efforts on common vulnerabilities and exposures (CVEs) that are confirmed to be exploitable, and execute runbooks that emulate the actions of adversarial advanced persistent threats (APTs) to validate true cyber survivability. In 2021, Rebellion, in partnership with the DON CIO Office, piloted Nova at the Naval Postgraduate School, which recently won a DON CIO award for the effort.

**BIO:** Clint Green is a senior technical architect at Rebellion. Immediately before joining Rebellion, Clint has 22 years of experience and served as a big data technical adviser for various Defense Department and intelligence community commercial clients. He has served in a variety of roles focused on big data, advanced analytics, AI/ML and national security. Certifications include CompTIA Security+, Google Certified Professional Data Engineer, Cloudera Certified Hadoop Administrator, EMC Proven Professional Technology Architect.

# Accelerate the Mission with Zero Trust Secure AI Access to the Edge

**Andrew Whelchel, Senior Solutions Engineer – Federal, Saviynt •**

andrew.whelchel@saviynt.com

## ABSTRACT

Speed is essential to enabling mission delivery. Artificial intelligence (AI) is a modern force multiplier for the digital-enabled joint force. AI enhances the warfighter through AI models running in secure cloud structures and by running in hybrid locations enabled for model execution and data analytics-based model adaptation at hybrid edge environments. For speed of safe access to both AI model applications and AI data analytics, secure AI access methods enable this needed speed and agility. These secure AI access methods provide rapid data access and reduce the cyber threat risk needed to move at the speed of the mission. The key to enabling and unlocking these capabilities for AI at the edge (and in the secure cloud) is identity access and matching identity to the resources associated with the AI access. When AI access binds to identity, this enables agility of AI resources from cloud to edge while maintaining security and risk reduction throughout the system. This solution paper highlights several key AI access to edge capabilities including:

- Understanding where the risk is (even if undiscovered) and where it will be
- Leveraging AI-informed awareness for faster decision actions and reduced risk decisions using zero trust and ICAM
- Integrating ICAM in zero-trust architecture for secure AI access for data access and model integration at the edge.

**BIO:** Andrew Whelchel (CISSP-ISSAP, ISSEP, CAP, CCSP, CSSLP) started in information security and IAM immediately after graduation from the University of Memphis and supports identity and access management managing Microsoft Identity for U.S. federal customers. He 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, federal and other customers, there was focus on identity risk analytics and integration of identity fraud intelligence for cybercrime prevention. Andrew, while at Okta and now at Saviynt, focuses on protecting employees as well as business partner identities for public sector agencies to reduce cyber risk and accelerate capabilities for cloud transformation. Contributions include work as a contributor on the National Institute of Standards and Technology 1800-3 ABAC (Attribute Based Access Control) standard and speaking events on identity access management and security.

# Making Zero Trust Work for You

**Kevin Brooks, Principal Digital Strategist, ServiceNow •**

kevin.w.brooks@servicenow.com

## ABSTRACT

Zero trust is what it sounds like—a security framework that operates on the tenant that no actor, system, network or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access. This is a dramatic paradigm shift in philosophy of how we secure our infrastructure, networks and data, from verify once at the perimeter to continual verification of each user, device, application and transaction. Contemporary threat actors, from cyber criminals to nation-state actors, have become more persistent, stealthier and subtle. They demonstrate an ability to penetrate network perimeter defenses with regularity. Traditional perimeter-based network defenses with multiple layers of disjointed security technologies cannot meet the cybersecurity needs of this threat environment. A transition to a zero-trust architecture (ZTA) is mandated by the Executive Order on Improving the Nation's Cybersecurity and steps to get there are detailed in OMB memos and Department cyber guidance. But more than meeting a mandate, the transition to zero trust makes sense as a way to maintain a strong, secure cyber infrastructure while enabling digital modernization—critical for the success of our nation. Zero trust is not achieved with a single technology. Rather, it is dependent on multiple, complex technologies working together to provide the validation of trust in a way that is seamless to end users. It is an approach that requires cybersecurity teams to orchestrate multiple security solutions. This position paper examines the recommendations for implementing a successful ZTA to support mission operations, service delivery and employee experiences. We will focus on:

- A single enterprise inventory system or CMDB with IT and OT visibility
- Improved attack-surface management and security posture
- Improved remediation and patch management capabilities
- Leverage new machine learning and artificial intelligence capabilities where possible
- Automate, orchestrate and integrate security incident response and detection capabilities
- Integration of specialized 3rd party applications such as SASE, BYOD, MDM, CASB, Container Development, endpoint detection, threat intelligence feeds and Identity and Access Management platforms.

Enable Enterprise Managed Accounts OMB guidance directs agencies to ensure that federal staff have enterprise-managed accounts, allowing them to access everything they need to do their job while remaining reliably protected. Identity, credential and access management (ICAM) is designed to create a secure and trusted environment in which users can access authorized resources. ICAM allows the agency to see who is on the network at any given time. The first step in zero trust is understanding what assets and systems are a part of your environment. Agencies must effectively catalog their digital assets and intellectual property in terms of potential risk and implement procedures to identify, manage, and monitor the users, devices, and applications accessing this data.

**BIO:** Kevin is a seasoned professional with more than 28 years as a military and federal leader of organizations and teams who builds large-scale transformation initiatives. He has a proven track record of leveraging his skills to implement people and process solutions that increase satisfaction and drive growth. During his career, he has served in increasing levels of responsibility while leading and developing high performing teams of cross-functional experts in challenge environments. Kevin was the functional implementation lead of an Air Force-wide updated of the MyPers (HR) system, moving the platform to the Oracle Service Cloud and posturing it for future expansion as a modern HR system. While serving as career field manager for the U.S. Air Force Force Support personnel, he championed the development of a more analytics savvy workforce across all levels of operations to better leverage emerging gains in predictive analytics and data focused decision making.

# Quantum-Resistant Security

**Bill Becker, Chief Technology Officer, Thales TCT** • [mary.shiflett@thalestct.com](mailto:mary.shiflett@thalestct.com)

## ABSTRACT

Quantum computing is advancing rapidly, and its impact is likely to render today's encryption algorithms obsolete. Quantum computers can launch attacks that break asymmetric cryptography, rendering the entire PKI-based encryption method obsolete. In fact, the National Institute of Standards and Technology is researching ways to deal with the effects of quantum power. As quantum technology advances, agencies will be forced to protect their information and communications against cryptographic attacks through quantum resistant technology. Thales TCT offers how to stay one step ahead of the quantum risk by deploying future-proof encryption technology to protect your data and offers:

- Overview of the security risks posed by quantum computers
- National quantum initiatives
- Crypto agility

**BIO:** Bill Becker is Thales TCT's chief technology officer (CTO). Bill is responsible for the company's technical vision and product strategy. As CTO, Bill leads Thales TCT's strategic initiatives associated with the development of innovative cybersecurity solutions to meet the needs of the company's U.S. federal government customers. Bill also works directly with the company's customers and technical partners to evaluate emerging technologies. Bill has spent nearly 30 years developing technology in support of cybersecurity and government initiatives. He has been with Thales TCT (formally SafeNet Assured Technologies) since its creation in January 2015. Previously, he spent 18 years with SafeNet, Inc., most recently serving as a technical architect in the CTO's office. In this role, he supported government-related business by focusing on transitioning traditional data security products to new virtual and cloud-based architectures. Bill has also held positions at Northrop Grumman, where he specialized in the development of fighter jet radar.



# Zero Trust: Beyond the Buzzword

**Bill Becker, Chief Technology Officer, Thales TCT •**

mary.shiflett@thalestct.com

## ABSTRACT

Zero Trust is not just another buzzword in a never-ending list of tech trends. The principles of zero trust eliminates the binary trust/don't trust approach applied to users and assets in yesterday's on-premises, perimeter-centric environments. According to a recent survey, 100% of U.S. federal government agencies are storing sensitive data in third-party cloud, mobile, social, big data and Internet of Things platforms, which inherently makes data vulnerable. Traditional perimeter protection does not protect off-premise data, which speaks to the need to take a zero-trust approach to data security. In fact, the White House has even issued guidance including the Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and intelligence community Systems and Executive Order 14028, which require agencies to develop a plan to implement a zero-trust architecture (ZTA). This paper discusses the best practices for implementing a ZTA to protect your most sensitive data and offers the top five things you need to know about zero trust:

- The basics. What is zero trust and how does it apply to data security?
- Setting the stage. How digital transformation can make data vulnerable but also more secure.
- Getting to work. Tips for putting ZTA into action.
- What about the cloud? How does cloud make implementing zero trust faster but more complicated?
- Pulling it all together. How to develop a long-term strategy to protect data throughout its lifecycle that maps to guidance such as CISA Zero Trust Maturity Model, OMB Zero Trust Strategy, DoD Zero Trust Reference Architecture, and NIST Zero Trust Architecture.

**BIO:** Bill Becker is Thales TCT's chief technology officer (CTO). Bill is responsible for the company's technical vision and product strategy. As CTO, Bill leads Thales TCT's strategic initiatives associated with the development of innovative cybersecurity solutions to meet the needs of the company's U.S. federal government customers. Bill also works directly with the company's customers and technical partners to evaluate emerging technologies. Bill has spent nearly 30 years developing technology in support of cybersecurity and government initiatives. He has been with Thales TCT (formally SafeNet Assured Technologies) since its creation in January 2015. Previously, he spent 18 years with SafeNet, Inc., most recently serving as a technical architect in the CTO's office. In this role, he supported government-related business by focusing on transitioning traditional data security products to new virtual and cloud-based architectures. Bill has also held positions at Northrop Grumman, where he specialized in the development of fighter jet radar.

# Security From Compliance within a Zero-Trust Architecture

**Keith Driver, Chief Technology Officer, Titania Ltd.** • keith.driver@titania.com

## ABSTRACT

There are many aspects to zero trust, but at its heart lies the principle that no entity should be implicitly trusted due to the application, device or location that they appear to be using. The second principle is to understand your estate and ensure every node in the network is configured correctly and has no security holes. As networks mature toward higher levels of zero-trust implementation, it becomes necessary to ensure that the network remains secure and that any inadvertent or deliberate acts are discovered quickly, and the risk remediated. However, what is deemed to be secure today may not be tomorrow. Configuration drift is a perfect example of this, where network engineers make changes to meet operational requirements. For example, routing changes or firewall rules, resulting in device configurations drifting out of compliance with policy, bringing about unintended security vulnerabilities. While most of this activity is benign in intent, it could potentially lead to critical security and operational risks nevertheless. This is why network and security teams need continual assurance that the actual state of the network reflects the desired state. Titania's innovative approach to this challenge is a solution, Nipper Enterprise, with the capability to accurately automate security and compliance assessments of every networking device—router, switch and firewall—in a network on up to an hourly basis, ensuring that any misconfigurations are identified quickly and remediated as soon as practicable. Nipper Enterprise's unrivalled accuracy in configuration assessment, which is delivered by virtually modelling devices as opposed to scanning them, ensures that users have the confidence and the assurance that their networking devices are performing as intended and reduces alert fatigue resulting from false positives. Deviations from configuration baselines that create security vulnerabilities are contextualized by Nipper Enterprise with risk-related information, such as impact to the network and ease of exploit, as well as recommended remediation fixes, thereby informing any remediation workflows or POAMs. Additionally, these findings data can be used to reflect a network's compliance performance against trusted RMFs, such as NIST 800-53 or NIST 800-171. As stated in the DOD's zero-trust architecture, a core tenet of a zero-trust environment is determining the compliance state of the network according to existing hardening standards and then ensuring that networking devices are managed and compliant with these standards, and Nipper Enterprise represents an innovative and effective way to realize this principle.

**BIO:** Keith Driver joined Titania as chief technology officer (CTO) in February 2019 from his role as an engineering fellow and CTO Cyber at Raytheon UK. He has a distinguished career in the telecommunications and security industry as a technology leader and board member in a variety of subject matters and large organizations, delivering revenue growth and technical advantage through strategy definition and innovation. Keith has worked extensively with commercial-, defense- and government-sector customers globally, and has spoken regularly at global conferences.

# RPA in the SOC: Human-Machine Teaming for Threat Response

**Bill Nystrom, Defense Cyberspace and IT Automation Leader and Strategist,  
UiPath • lorna.joseph@uipath.com**

## ABSTRACT

Cyberattacks unfold at machine speed, leaving smaller and smaller windows for effective security operations center (SOC) response actions as technology evolves. More than 33% of all cyberattacks are fully automated, often leaving only minor target and timing variables to the adversary to customize. However, at stark contrast, security teams are often forced to face these automated attacks with many manual and repetitive processes that significantly hinder speed of action. While many SOCs possess the latest cybersecurity threat detection, remediation and response tools, there is often an automation gap that leaves hundreds of people-centered processes meandering throughout the typical end-to-end cyber defense workflow. A simple and practical implementation of robotic process automation (RPA) capabilities integrated into the cyber defense workflow can level the playing field and allow for faster prevention and response for new and previously unknown threats as they are discovered, profiled and confronted by security teams. RPA can enhance and augment security teams in multiple forms in various scenarios: Attended RPA can be paired with analysts to perform tandem and human-in-the-loop response actions at higher speeds with more context and agility that purely manual or automated workflows may struggle to process alone. Additionally, unattended RPA can constantly monitor for triggers, tips and queues poised and ready with way playbook of options. RPA can also be positioned to bridge API and log gaps for legacy systems while enabling dynamic expansion of sensor coverage based on threat-levels. When used in tandem, both attended and unattended RPA can work collaboratively with a SOC analyst to take speed the end-to-end threat response cycle.

Additional actions that RPA can take in the SOC are:

1. Automatically deploy security controls when inconsistencies are discovered between systems.
2. Classify the virus alerts according to threat categories.
3. Trigger a security control based on the detected alert.
4. Generate a summary report of the threat and send it to the cybersecurity team.
5. Open an incident ticket with the IT service desk and ITSM for indexing.
6. Notify key stakeholders of SLA timelines at interval

This discussion paper lays out the key points in integrating RPA into an active SOC so threat analysts can spend less time collecting and manipulating threat data so they can focus on more advanced tasks in the response cycle.

**BIO:** Bill Nystrom is Defense Cyberspace and IT Automation leader and strategist. At UiPath, he is responsible for providing global aerospace & defense industry depth and relevance in support of automation growth and adoption across defense portfolios. He provides subject matter expertise to expand human-machine interoperability to speed operations. Bill is a 22-year veteran of the U.S. Air Force, having filled various Cyberspace and IT roles across the force.

# Cybersecurity in the Age of Zero Trust

**Mike Malaret, Technical Director, U.S. Public Sector, Veritas Technologies •**

mike.malaret@veritas.com

## ABSTRACT

As cyber threats against organizations increase and evolve, traditional “trust but verify” network cybersecurity approaches are no longer enough to deter attacks and protect data and systems. Zero trust allows organizations to implement better access control, contain breaches, protect their assets and mitigate the potential for damage. However, without a carefully planned architecture and strategy, it all might end up wasting efforts and resources. As part of an organizations zero-trust approach, they should focus on immutability, resiliency and keeping up to date with patching. Without a concerted effort at security and resiliency, organizations can be in a culture of zero trust and still be vulnerable. The Veritas Technologies suite of products have embodied multiple layers of zero-trust principles for years and are architected to enhance the zero-trust architecture for customers. Veritas highlights solutions that provide a unified, multi-layered platform approach to seamlessly integrate intelligent protection, comprehensive detection and industry-leading backup and recovery.

**BIO:** Mike Malaret serves as the Veritas Technical Director for the U.S. Public Sector. He is responsible for leading business and technical operations, including technical positioning, alignment and development of technologies relevant to the defense and intelligence communities. His scope covers providing advice on topics covering cloud, big data, critical data protection, data security and infrastructure visibility. Working with the Veritas Product Security Group, Product Management and Engineering, Mike has been instrumental on building out Veritas’ Federal Government Security and Compliance practices.

# Zero-Trust Architecture for Mission-Critical Operations: From Sensor and Cloud to Tactical Edge

**Nicholas Lessen, Solutions Architect, Forcepoint •**

[brittany.williams@forcepointgov.com](mailto:brittany.williams@forcepointgov.com)

## ABSTRACT

Multi-cloud environments are providing solutions for high velocity and a high volume of information exchange, but caution: Cloud, on-prem applications, and implementing zero-trust architecture (ZTA) might leave entities vulnerable to attack. For zero trust to be truly operational and support secure collaboration wherever needed, consolidation is required: converging identity solutions, new capabilities and integrating behavioral analytics in a continuous fashion. Success of zero trust hinges on the new insights that these converged technologies offer security teams. Forcepoint explores integrating human factors into security systems and processes, showcasing combined strengths of multiple technologies and behaviors across users, devices, applications, content and data. Learn how a converged architecture of multiple capabilities can simplify and reinforce cybersecurity far beyond traditional perimeter defenses. Even in air-gapped, isolated network environments. An effective ZTA drives agencies toward a more data and user-centric approach while moving beyond the perimeters of old. It incorporates user identification and behavioral analysis, attack surface mitigation, and data management for continuous and adaptive Zero Trust. With these elements, agencies can meet the Biden Administration's goal to "identify, deter, protect and respond" to cyber threats, support defensive cyber operations and DCO Enclaves, and achieve RTB, JADC2, while remaining compliant.

**BIO:** Nicholas Lessen is a solutions architect specializing in user, entity and behavior analytics at Forcepoint, a leading user and data protection cybersecurity company. Nicholas has been a trusted adviser to the federal government for more than two decades, designing and implementing technical solutions. Nicholas is a CISSP and a Capella University PhD candidate.

# A New Approach to Modernize Your Zero-Trust Architecture

**Steve Ryan, Founder and CEO, Trinity Cyber Inc. •**

jessica.johannes@trinitycyber.com

## ABSTRACT

Just as Mark Twain is famously misquoted as saying to a reporter “The reports of my death have been greatly exaggerated,” the concept that zero trust has made the edge irrelevant and that “the edge is dead” are similarly inaccurate. While zero trust is a step in the right direction, it does not account for threats from the Internet or the urgent need to secure Internet traffic. The Internet-facing network edge and connections to the Internet remain most vulnerable for organizations, and adversaries who continue to successfully exploit this exposure. They will continue to do so unless a modern zero-trust architecture is deployed. To realize the full benefits associated with zero trust and protect against today’s cyberattacks, the modern zero-trust architecture must include the ability to identify and automatically defeat the methods adversaries employ as well as individual threats is crucial to securing the network edge and protecting Internet traffic. Traditional technologies such as IPS fail to provide adequate security for the network edge and Internet traffic because, like building a structure on sand, the underlying technologies that make up the foundation are not up to the task of identifying and preventing today’s sophisticated cyberattacks.

Adversaries have considerable knowledge of how to outmaneuver and avoid detection from existing security infrastructure systems. Reasons for this include:

- Over reliance upon approaches that are well understood by attackers such as static indicators of compromise (IOCs) and rudimentary signatures
- Inability to deeply and contextually interrogate the contents of network traffic resulting in many alarms and false positives that overwhelm stretched and overburdened security operations center resources
- Restricted preventive control capabilities of only block or allow, as well as inability to address corrupted traffic Instead of playing a continuous game of “Whack-a-Mole” against individual cyberattacks, what’s needed is new innovation to evolve the zero-trust vision.

To secure the Internet-facing network edge and protect Internet traffic, the ability to identify, defeat and prevent threats with extreme accuracy and speed before the threats enter or leave the network is critical to delivering ongoing protection from modern cyberattacks. A breakthrough technology is now available that uniquely delivers the innovation needed to realize fully zero-trust protection and benefits. It deeply inspects and modifies Internet traffic in a contextual manner, at speed and scale to identify and detect threats other technologies miss. It uses powerful new actions beyond block and alert such as remove, modify and replace to provide precise levels of threat prevention and neutralization before threats can interact with the network. Government entities, critical infrastructure providers and enterprise customers across many industries are already experiencing the benefits of this powerful new technology.

**BIO:** Steve Ryan is founder and CEO at Trinity Cyber, Inc. A recognized leader in cybersecurity, Steve served as the Deputy Director of the National Security Agency (NSA) Threat Operations Center (NTOC) after a distinguished 32-year career as a custom chip designer and cybersecurity operator. He was a primary architect of the NSA's NTOC, bringing together intelligence and defensive missions to identify and stop cyber threats at very large scale. Steve excels in challenging the status quo to developing unique solutions to the world's most complex problems. He has applied his unique skills and vision to develop Trinity Cyber's fundamentally new approach to cybersecurity. Steve holds a Bachelor of Science degree in electrical engineering from the University of Rhode Island.

# Cyber Forza Zero-Trust Compliant Architecture Implementation and Case Study

**Dr. Venkat Rayapati, Founder and CEO, Cyber Forza, Inc. •**

vrayapati@cyberforza.com

## ABSTRACT

In this paper, Cyber Forza provides an enterprise zero trust architecture (ZTA) implementation with use cases. Cloud Security Posture Management with current threat landscape challenges are addressed. CyberForza Integrated Cloud Cyber Defense Platform defends the impact of security breaches on the organizations and reduces the risk of mission-critical data loss. How to implement zero trust and Presidential Executive Order 14028 compliances are discussed. ZTA implementation and risk mitigation benefits are addressed for the on-premise, hybrid and cloud deployments. Multi-cloud zero-trust deployments security breach risk reduction emphasized. CyberForza Zero Trust Implementation for the enterprise case study results are presented. Enterprise CISOs and CIOs today face tougher challenges than ever. The threat landscape has expanded exponentially, while security teams are forced to work within tighter budgets and meet the demands of all the stakeholders within the organization. This paper provides the details of the CyberForza ZTA implementation for enterprises and benefits. Presidential Executive Order 14028 on modernizing and improving cybersecurity, with the zero-trust model of security has become increasingly important for organizations seeking to protect their networks, data and applications. In practice, the zero-trust model is typically implemented in the form of security policies, whether via micro-segmentation, web gateways or least-privilege access control. In this connection, it is often associated with the Secure Access Service Edge (SASE), SD-WAN and other security and networking services designed to accommodate the new digital transformation of business. While particular implementations will vary, the zero-trust model generally uses these services as a coordinated mechanism that allows the minimum access required to accomplish business objectives. CyberForza Zero Trust Eagle Platform complements and enhances zero trust postures for cloud, on-premise and hybrid deployment environments with self-learning artificial intelligence that identifies, interrupts and investigates unpredictable cyber threats that get through, even if they operate over legitimate paths. This includes advanced external attacks like ransomware, zero-days and supply chain risks, as well as compromised, careless or malicious insiders with privileged access. The continuous monitoring with threat management is adaptive in its understanding and pervasive in its scope, delineating normal and abnormal patterns across outsider, insider, user, critical data, networks, applications, cloud, remote endpoints, IoT, and the corporate network. CyberForza Zero Trust Architecture Integrated Cyber Defense Platform brings the following benefits:

1. CyberForza Zero Trust Defensive Layer designed to protect distributed networks via access policies and a cloud security posture management.
2. Zero Trust Defensive Layer will defend against attacks that can be identified by policy-driven detection mechanisms.
3. Complements with CyberForza Integrated Cyber Defense Platform that detects, defends and responds to zero-click, zero-day, advanced malware, ransomware threats and interoperates with existing legacy security.
4. Multi-cloud zero-trust data protection and risk mitigation provided through data base level intelligent migration CyberForza Zero Trust Eagle Platform - Integrated Cyber AI Defense Platform will provide "fastest detection" zero-trust compliance implementation for enterprises



**BIO:** Dr. Venkat Rayapati founded the Cyber Forza, Inc. Prior to that, he worked as president and CEO of SAI Technology. He worked as vice president of design engineering at Global Foundries. He served as chief technology officer & chief operating officer of Xalted Networks, Inc. Venkat also co-founded Portal Player Inc. (now part of NVidia) as its vice president of engineering & CTO. He worked on the NASA Space Station several satellites, and advanced DOD projects. He has more than 20 years of experience in cybersecurity, wireless technology and artificial intelligence. He has worked at Lucent Technologies (Bell Labs) as director of product development. He won the Bell Labs President Award for the Stinger and Eagle Product Innovation. He held senior technical positions at Nortel Networks, National Semiconductor (chief architect) and AMD (architecture manager of K6 &K7). Venkat was also on the Board of Directors at Digital Video Systems, Inc. He holds a PhD in electrical and computer engineering from the University of Montreal, Canada. He worked as a visiting professor at Stanford, UC Berkeley and UC Santa Cruz. Venkat has published approximately 35 papers in various reputable international journals and spoken at many conferences.

# Aligning ICAM, the Executive Order & Zero Trust for the Defense Department

**Josh Brodbent, RVP Public Sector Solutions Engineering, BeyondTrust •**

escanlan@beyondtrust.com

## ABSTRACT

In our rapidly changing digital world, agencies must evolve security strategies. A goal of zero trust is to create a security and network architecture that is dynamic, adaptable and protected. The Executive Order on Cybersecurity has moved the term “zero trust” from a buzzword to a much-needed mindset shift in how we secure agency data and systems. Agencies must leverage zero-trust principles to never trust, always verify, and only allow access when contextual parameters are met. Identity sits at the heart of zero trust. In a perimeter-less world, agencies must think through ways to prove an identity for access to stop adversaries from getting in and ultimately from moving laterally within an environment. Leveraging ICAM and robust identity security strategies enables agencies to move from a network-based approach to a data centric approach to defending systems. Join BeyondTrust and government security experts for a discussion to understand:

- Why Privileged Access Management (PAM) is essential to major DOD initiatives such as ICAM, Thunderdome and zero trust
- How ICAM supports the Executive Order and the Defense Department’s outlook on data centric security and defending agency systems
- The path to secure modernization using least privilege

**BIO:** Josh Brodbent has more than 20 years in IT experience and has architected identity and privilege access management solutions for more than 3 million user accounts. He joined BeyondTrust in 2018 as a senior solutions engineer and was quickly selected to lead the team. Prior to BeyondTrust, Josh was a senior solutions architect for Quest Software. He began his career by founding a managed service provider (MSP) at 12. He held multiple industry certifications by 14, making him the youngest in the nation to do so. That MSP went on to become successful, and ultimately his launching point into public sector architecture and support.

# RMF Acceleration through eMASS Automation

**Brian Hajost, Founder and Chief Operating Officer, SteelCloud •**

[jcoffey@steelcloud.com](mailto:jcoffey@steelcloud.com)

## ABSTRACT

Enterprise Mission Assurance Support Service (eMASS) acts as a repository uniting technical/machine data generated from endpoint scans with the human/non-technical data documented by security/IA personnel. Traditionally, this “uniting” process is accomplished by completing a STIG viewer checklist for each policy for each endpoint, quickly generating a cumbersome number of hand-created checklist files. With these overwhelming manual processes, keeping eMASS current is a challenge, creating security issues that could hobble your organization. Brian Hajost shows you how you can accelerate RMF, keep eMASS up to date and ensure compliance through automation. Learn ways to:

- Automate and reduce the effort and errors in merging non-technical data with machine-generated technical data
- Automate and simplify the production and input of compliance data into eMASS
- Automate and reduce the effort to produce, name and store fully populated STIG viewer checklist in bulk (by the 1,000s)
- Provide complete CKL data to SIEM data feeds so that complete compliance data is easily accessible through integrated enterprise dashboards

With cybersecurity growing more complex by the day and regulations in constant flux, automation is the only option for an efficient, effective, exacting security approach.

**BIO:** Brian Hajost is the founder and chief operating officer of SteelCloud, a company that develops technology for automated remediation of endpoints to the DISA STIGs and the CIS Security Benchmarks. Brian has transformed SteelCloud into a recognized pioneer in delivering new technologies that allow government customers and commercial enterprises to effectively meet the compliance mandates of RMF, DIACAP, NIST 800-53, NIST 800-171, and IRS Pub 1075. Brian’s technical career has spanned more than 30 years, primarily with leading-edge technologies in regulated industries. He holds three patents in IT security and two patents in mobile security. Brian is an active contributor to AFCEA’s Washington, D.C. Chapter, currently serving as vice president and a board member. Brian is also a member of AFCEA’s Technology Committee.

# Extensible Zero-Trust Framework at the Digital Edge

**Don Wiggins, Global Chief Solutions Architect, Equinix •**

dwiggins@equinix.com

## ABSTRACT

For a decade or more, digital transformists have begun their respective journeys in cloud adoption at the digital edge—a place where agencies continue to establish geo-strategic, globally distributed proximal adjacency to a growing field of cloud and other digital service providers. Early adopters did so largely in remote fashion by leveraging, in many cases, their ISPs to connect to a cloud provider. As testing and trials of cloud services progressed to mission-critical production workloads, often evolving to hybrid multi-cloud environments, it became readily apparent that ensuring service symmetry, low latency and equitable service distribution across ever-increasing, geo-disparate user communities necessitated a new architectural approach. Centralized core, network centric architectures continue to yield to a more application-centric, regionally distributed approach—optimizing alignment with services consumed where the mission dictates it. This approach implies that agencies thoughtfully and securely extend their existing network boundary (or service providers on behalf of large government agencies) to locations proximal to the many thousands of digital service providers that are leveraged for various agency initiatives, use cases, etc., where proximal access to a global carrier-neutral ecosystem of thousands of API-integrated digital service providers can be leveraged in a regionally distributed aggregate.

That traditional security boundary built around an on garrison-based enclave by way of a north/south, ingress/egress point is now being extended to interconnection platforms like Equinix where they can readily access and privately peer directly with myriad service providers and/or mission collaborators. This recently adopted tactical digital edge location has become the nexus for a growing number of highly adaptive cloud adjacent and cloud native use cases that enable streamlined, frictionless, rapidly provisioned interconnection and collaboration and the point of transact. Extending that boundary while adding authorized access to a growing number of regionally distributed hybrid multi-cloud environments and inter/intra agency collaborators requires a higher level of sophistication and scale as it relates to an extensible, modernized security framework. Equinix has remained engaged, consultatively with the federal government with two key initiatives that align with this new architectural approach, specifically a modernized trusted Internet connection (TIC) as an integral component to a broader zero-trust framework that can more holistically qualify and quantify access to a more diverse/collaborative and geographically disparate use community. Cybersecurity analytics, much like the digital assets and sensitive information it is employed to protect must continue to evolve and account for this new digital landscape. Beyond credentialed access, interdiction of increasingly more sophisticated adversarial exploits will require a more holistic approach to cybersecurity. Adaptive, behavioral cognizance of user access, for example becomes a critical attribute of a broader security framework and can be addressed with the implementation of AI/ML-enabled cybersecurity solutions that gain cumulative behavioral awareness of authorized users. A common analogy might be, for example a U.S. bank customer who, while abroad on vacation, attempts to access their bank account from a foreign country. The AI/ML-enabled cybersecurity platform can quickly qualify and/or challenge the access as appropriate.

**BIO:** Don Wiggins is the chief global solutions architect for Equinix's Government Solutions Information Technologist, where he's been since 2013. A veteran, Don had a 21-year career with the U.S. Air Force and has nearly 20 years as an IT consultant. He is the founder of two IT consulting firms, both with a focus on the public sector, and is experienced in a broad spectrum of IT consulting engagements with a primary focus on digital transformation. He is uniquely positioned to provide deep insights into current trends in technology innovation that translate into measurable cost savings, operational efficiency and mission execution. He serves in a trusted advisory role facilitating a strategic partnership between the public sector and the technology industry.

# Future of the Edge: Overmatch for Secure Edge Platforms

**Brad Sollar, Chief Technology Officer, Mainsail Industries •**

brad@mainsailindustries.com

## ABSTRACT

To face advanced adversarial threats, warfighters will need to leverage edge cloud computing on the battlefield or tactical edge that are able to operate in denied, degraded and cyber-hostile environments. How can organizations such as the Defense Information Systems Agency (DISA) keep up with the growing amounts of data being produced and collected at the edge and keep that data secure? Centralized data processing in DOD clouds has brought many benefits but can present multiple challenges when dealing with distributed and tactical edge computing. Orchestrating (multi-domain) data back to a centralized data center where AI/ML data processing can process and make decisions comes with many obstacles. Getting answers from AI/ML applications in the cloud out to commanders in-theater where they can make use of the information to assist in real-time decisions can present challenges in moving and securing data. Data must be replicated and synchronized between hyper-scale clouds and many dynamic tactical edge nodes, where the network pathways suffer from disruption, latency and single points of failure. Networks will have to be able to deal with intermittent connected/disconnected network states. This becomes even more challenging when multiple levels of data security are introduced where data needs to be orchestrated and secured through multiple cross-domain devices.

New security protections will be needed when multiple levels of classification are produced and collected on the same edge platform. Edge platforms by nature will be a constant target by adversaries to infiltrate, deny or disrupt. Edge platforms not only have to counter traditional software-based cyber threats but must be resistant to physical data extraction attacks on the platform as well. Bringing AI/ML workloads to the edge has many benefits for warfighters, such as enhancing decision-making in-theater and reducing the dependency on an intermittent network that might not be there. Processing data at the edge allows sophisticated situational awareness applications to deliver answers to commanders in real-time and be self-sustainable while on the move. To solve the expected cyber, denial and degraded communications problems expected in a near-peer environment, systems will need to be able to deal with workload resource contention and quality of service levels needed to run AI/ML applications locally and deal with full-stack cyber protection and controls from the hardware up to the application.

Our team is leveraging more than 20 years of engineering expertise in building secure weapon systems and multi-level security & cross-domain systems engineering from their combined tenure at places such as Lockheed Martin, Johns Hopkins University Applied Physics Laboratory, MITRE and Red Hat. Our team has solved many of the problems surrounding edge platform quality of services for workloads as well as hardware & software cybersecurity. With our adversaries' growing cyber and AI/ML capabilities, the threat against our warfighters becomes more of a realized threat, especially against edge platforms. Increasingly, warfighters face global threats and need the flexibility to deploy edge platforms wherever they are needed and have the confidence that they are secure and operational.

**BIO:** Brad Sollar was an U.S. Army 35D radar technician for Air Traffic Control Systems, where he learned to build networks and secure engineering. Brad worked at Raytheon protecting homeland security and DOD networks as an IDS/SEIM analyst. He then moved from defensive to offensive cybersecurity while at Lockheed Martin, working with INSCOM/ARCYBER. While at Red Hat he worked with emerging technologies such as OpenShift//Kubernetes and spoke frequently on cloud and container security. Currently, Brad is the chief technology officer of Mainsail Industries, which focuses on secure edge computing for the DOD.

# Deploying Multi-Mission Workloads at Scale

**Jason Strawderman, Senior Director of Sales and Business Development,  
Facility Security Officer and Co-Founder, Western Digital Federal •**

jason.strawderman@wdc.com

## ABSTRACT

As workloads and services move to public cloud infrastructure, we gain efficiencies of scale by centralizing our services. But, a global force, changing network conditions, real-world events and evolving threats can necessitate the movement of workloads closer to the edge to enable high availability of services. The Defense Information Systems Agency (DISA) needs approaches that intelligently move workloads from central cloud locations to edge computing environments on-demand to enable secure multi-mission workloads and to facilitate the best user experience. What's needed is a militarized and ruggedized high-performance edge platform that enables organizations to rapidly deploy remote data capture and analytics at the cloud edge. Processing data at the tip of the spear reduces the latency associated with sending data from a remote location to the core for processing. Remote processing reduces the amount of traffic on network backbones, delivers on-site analytics and enables faster decision making. Edge locations can rely on data center cloud-like services even when a network connection may be insecure, intermittent or non-existent. The remote server can enable applications that normally runs on IaaS environments to be run remotely. Edge solutions must be capable of stacking to enable the creation of remote compute clusters, and it should be resistant to security threats such as external electromagnetic events and detection during sensitive operations. Of course, the edge server must be designed for harsh environments to protect against failures induced by shock and vibration during transit. We introduce you to how a vertically integrated manufacturer such as Western Digital has approached these challenges to deliver a world-class edge-server to meet the demanding needs of remote deployments.

**BIO:** Jason Strawderman serves as the senior director of sales and business development, facility security officer, and co-founder of Western Digital Federal. Since joining Western Digital in September 2017, Jason has focused on establishing Western Digital as the leading data infrastructure producer serving the U.S. government and the defense industrial base complex. With more than 40% of the world's data stored on its products, Western Digital solutions power innovation from the devices we use every day, to the foundation of cloud infrastructure and to the edge. Previously, he served in sales, marketing and business development leadership roles at leading data infrastructure companies such as Tegile Systems, Hewlett Packard Enterprise, LeftHand Networks and Quantum Corporation.



# Distributed Zero-Trust Security

**Kim Van Der Wende, Field & Channel Marketing Manager – Federal, Palo Alto Networks** • kvanderwende@paloaltonetworks.com

## ABSTRACT

There are several technical and mission advantages associated with using the Palo Alto Networks portfolio of solutions to achieve a zero-trust architecture: Optimize the user experience and access to cloud-based and internal applications without sacrificing security or performance. Deliver a consistent user experience and security for all users and devices, no matter where they reside—whether they are on premises, remote or roaming between locations. Enforce consistent security compliance across all users, devices and applications throughout the DOD enterprise and make it easier to identify all traffic by user, device and application through a consistent set of visibility and control mechanisms. Obtain complete situational awareness of end-user and device posture, application and activity—legitimate and otherwise. Implement all zero-trust principles and concepts, including enforcement of policy through a single management console (see the DOD Zero Trust Reference Architecture, Section 1.4.1: Produce Consistent Policy) and a distributed zero-trust perimeter for tactical and mobile assets, coalition environments and DOD public cloud computing resources.

Instead of trusting users and their devices to do the right thing, the security model verifies that they are doing the right thing before allowing action and continuously monitors to ensure that users and devices are still doing the right thing. Leverage fully integrated content inspection tools to improve security and visibility into the network to thwart malware and lateral movement of threats. Reduce total cost of ownership using a consolidated, well-integrated security platform across DoDIN, instead of disparate collections of point products with varying levels of integration. The DOD already has much of the baseline infrastructure for zero-trust policy enforcement points (PEPs) and centralized policy management in place, as a result of its significant investments in Palo Alto Networks solutions. This provides an optimal framework in which DISA and DOD can begin to incorporate cloud-delivered PEPs. Palo Alto Networks was one of the vendors that participated in the DIU SCM pilot. Our portfolio allows an approach that includes a next-generation application-aware firewall, CASB capabilities, user- and device-based zero-trust application access, and a cloud-based secure web gateway. The overall portfolio is highly differentiated, as it is application-defined throughout all components. A centralized management console is used to create and manage policies and gain visibility into the zero-trust PEPs.

# Zero Trust Hardware Access

**Yossi Appleboun, CEO, Sepio** • social@sepiocyber.com

## ABSTRACT

The concept of zero trust is not new. It was first introduced in 1994, but, like anything, it takes a while for people to catch on. And, as the threat landscape continuously evolves, now, more than ever, is the time to start catching on. Typically, internal users and devices are automatically trusted. This is because it's assumed the secure walls of the enterprise are enough to keep out malicious criminals. A rookie error that IT departments are becoming increasingly concerned about, hence the desire to adopt zero trust. The model grants access based on who, what, when, where and how. If the organization cannot answer these questions accurately, then the zero-trust architecture (ZTA) is essentially ineffective. To answer such questions and have a strong ZTA, enterprises must have complete asset visibility. With zero-trust hardware access, the focus is on all hardware assets operating within the enterprise's infrastructure—including remote assets—as this is from where access requests originate. Concentrating on hardware improves the overall efficacy of the enterprise's ZTA, especially micro-segmentation efforts, as the PE can make accurate access decisions through deep visibility into a device's characteristics. Furthermore, enabling hardware access control through policy enforcement stops a hardware attacker at the first hurdle, not even giving them the opportunity to cause damage or infiltrate the network. Today, a qualified attacker could easily bypass existing security measures, even when ZTA is in place. Just think of a passive network tap inline to a sensitive network element or a MiTM spoofing attack tool which presents the façade and behavior of a legitimate device. ZTA relates to device identification and risk scoring, but how do you turn these guidelines into usable technology? The solution may lie in using new data sources previously not used—the physical layer (L1) the actual physical, electrical presentation of a given hardware asset. The next step in embracing zero trust would be validating devices' physical layer information, verifying and revealing the device's true identity, not simply what it claims to be, but what it is actually physically is. This would serve as a counter measure to attackers spoofing and rogue devices implanting efforts. By comparing and validating a device's physical layer digital fingerprint, true device trust could be achieved as conceived by the zero-trust concept founders.

**BIO:** With more than 25 years of experience in security, networking, computer science and control systems, Yossi Appleboun brings wide angle vision on cybersecurity. In the early 90s, after graduating from studies, Yossi joined the Israeli Army Intelligence (unit 8200) and served as a team leader and chief architect focusing on design and development of critical infrastructure network monitoring and security systems. In 1998, he was one of the founders of WebSilicon, an Israeli company that focused on delivering networking and security systems. As the vice president of R&D, Yossi was involved in design and implementation of more than 250 systems for government agencies, integrators and vendors. In 2013, WebSilicon was acquired by Magal (NASDAQ: MAGS), one of the world's largest physical security integration companies. After the acquisition, Yossi was tasked with leading the integration of his company into the Magal group, which included the rebranding of WebSilicon as CyberSeal. He served as the chief technology officer for cybersecurity of Senstar, Inc., the North American division of Magal, and relocated to the United States to work more closely with key customers and partners. In 2016, Yossi co-founded Sepio Systems.

# DOD Edge 2.0

**Michael Rau, Senior Vice President of Solutions Engineering and Enablement,**

**F5** • disa@f5.com

## ABSTRACT

Edge computing provides the opportunity to transform DOD application delivery, offering localized data analysis, artificial intelligence, process automation and other digital capabilities. This contrasts with current GovCloud-based infrastructure offerings that rely on centralized architectures built only on U.S. soil. The drawback of centralized architectures is that they cannot cost effectively support the ultra-low latency and extreme throughput demanded by localized workloads at the edge. Instead, cloud capabilities should be localized at the source of business data to form an edge cloud, which places computing, storage and networking resources where the data is sourced—at the edge of the network. An edge cloud capable of securely extending existing DOD cloud solutions, whether in GovClouds or on-prem, to the edge would create a fundamental DOD asset for innovation, enabling information dominance and transforming DOD business processes.

F5 Distributed Cloud Services (XCS) is an innovative new platform that can provide this solution. It works in concert with on-prem DOD data centers and GovClouds to extend their capabilities to the edge. It provides a secure and distributed cloud environment to deploy, secure and operate applications across diverse edge environments, including O-CONUS, forward operating bases or even extending to sensors on airframes. Key capabilities include application and infrastructure management and secure connectivity across edge sites and GovClouds. XCS provides a cloud-native software stack that integrates compute, storage, networking and security for DOD components to manage their distributed edge workloads. XCS provides secure connectivity service that seamlessly connects edge sites to each other and to GovClouds with zero-trust and application-level security.

### Challenges Addressed

1. Complexity introduced by monitoring heterogeneous edge environments in different GovClouds and operating a fleet of distributed applications and data.
2. Creating consistent, standardized security policies and profiles of distributed infrastructure, apps and data across GovCloud and on-prem environments.
3. Delivery of reliable and high performing connectivity across edge and multi-cloud.

**Benefits Simplification of Edge Fleet Management and Operations:** SaaS-based deployment and lifecycle management of hardware and infrastructure software allows customers to focus on application software development.

**Integrated Security from Edge to Cloud:** Protect the fleet of edge infrastructure and apps from vulnerabilities and get real-time visibility and telemetry from edge devices. Secure connectivity across cloud and edge enables end-to-end situational awareness.

**Performance Optimization and Cost Reduction:** SaaS-based delivery of platform services, coupled with a high performance global network, significantly reduces the cost of deployment, operations and application downtime at the edge.

**BIO:** Michael Rau has been with F5 since 2015. Prior to F5, Mike worked at Cisco for 20 years in a variety of different executive-level capacities in Systems and Solutions Engineering, Technical Strategy, Product Development, and served as the Field chief technology officer for Cisco's Enterprise Networking and Security portfolio. At F5, he initially served as the vice president of global sales solution engineering and later became the senior vice president of solutions engineering and enablement. In this expanded capacity, Mike was responsible for F5's Public Cloud Alliances and F5's technology partnerships. He has been actively involved as the sales lead in all M&A activities for F5. He took a leadership role in F5's acquisition of NGINX and Shape, which included due diligence as well as the integration into F5. This experience led Mike to move into the role of senior vice president of corporate and business development. In this role, Mike helped develop the company strategy for entering the edge market and that work led to his leading the acquisition of Volterra as a next-generation edge platform. Seeing the shift in the importance of SaaS and Managed Services for SP and enterprise customers, Mike moved into his current role, where he is responsible for global sales of F5's Distributed Cloud Services portfolio. This portfolio includes application security services, edge computing and advanced fraud solutions.



## WHAT IS AFCEA?

We focus on cyber, defense, security, intelligence and related information technology disciplines.

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

