CHAIRMAN'S NOTE

Dear Friends,

As we transition from Summer to the Fall Season, there are common themes that touch the Missions we support across the Federal Government, both in the Defense and Civilian Sectors, domestically and overseas.

Those themes include Data Access, Reducing Operational Support Costs and Ensuring System Availability and Reliability, while leveraging existing infrastructure. Through innovative solutions such as the use of Dynamic Multipoint Virtual Private Network (DMVPN) technology, this has enabled out customers to reduce the number of WAN circuits at each site, allowing for operational improvement with cost efficiency and simplifying the enterprise network topology for supporting remote site connectivity.

We Stay focused to meet the challenges ahead of us, Supporting our Customers and Each Other.
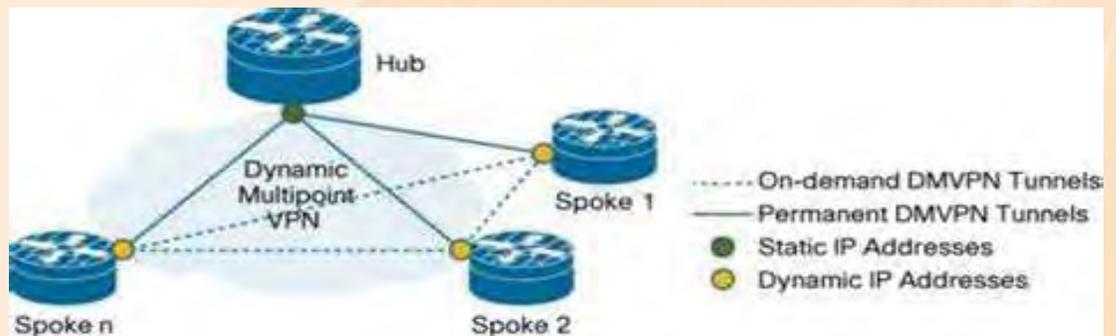
Ashley W. Chen

Founder & CEO

IN THIS ISSUE

Turning **VISION** into **ACTION**®

Ensuring Data Access and Reducing Operational Cost Through Innovative Network Solutions

By W. Paul Frazier, Sr. Program Manager

ctioNet works closely with our customers to leverage emerging technologies and network innovations that can help reduce cost while achieving Agency Missions. The key business outcome was to reduce remote site WAN circuit operational cost while maintaining the mission access redundancy required at each remote site. The Enterprise Network architecture coupled with security design requirements posed a challenge in presenting a solution that could be implemented without requiring a capital investment. We understood the challenge and the need to help reduce costs to allow funds to be moved to other Network Enterprise projects that are needed. After a deep analysis of the Enterprise Network Architecture and how the remote sites are connected, we were able to recommend a solution that would maintain network access redundancy failover and meet the security architecture requirements.

ActioNet serves as the Enterprise Network Design and Implementation support partner for Enterprise Infrastructure Engineering, delivering innovative network design solutions and Tier 3 troubleshooting support of network design changes implemented in our customers' environments. We recommended the use of a Dynamic Multipoint Virtual Private Network (DMVPN) solution that could leverage the already in-place architecture to reduce WAN Circuit dependency for redundancy. We designed the network topology and architectural diagrams to present to Technical Review Board highlighting the required changes, mitigation of performance risks, and compliance with Federal and Agency security requirements.

What is DMVPN? It is a Cisco networking solution for building scalable VPNs, particularly for connecting remote branch offices. It leverages GRE (Generic Routing Encapsulation) tunnels over IPSec encryption to create dynamic, on-demand connections between sites. DMVPN simplifies network management by using NHRP (Next Hop Resolution Protocol) to dynamically discover and build tunnels between spokes, rather than relying on static configurations.

"Reduced WAN operational cost by 50% with removal of multiple circuits at remote sites"

Ensuring Data Access continued from page 1

Our Network Engineers had to redo the IP Address scope at all the remote sites and Data Center connection points to implement the new network design. This allowed our customer to reduce the number of WAN circuits at each site, allowing for operational improvement with cost efficiency and simplifying the enterprise network topology for supporting remote site connectivity. Implementing the solution across 10 sites was completed in 5 months, which allowed the customer to go into the new fiscal year with lower operating costs.

BUSINESS OUTCOME

We implemented a seamless solution that provides the following benefits:
• Delivered a fully redundant network access solution to meet availability requirements.
• Reduced WAN operational cost by 50% with removal of multiple circuits at remote sites.
• Simplified operational monitoring of sites and updated monitoring rules for design.
• Improved availability with dynamic tunneling to reduce underutilization of bandwidth.
• Solution met the Zero Trust Architecture Security and 99.9% Availability requirements.
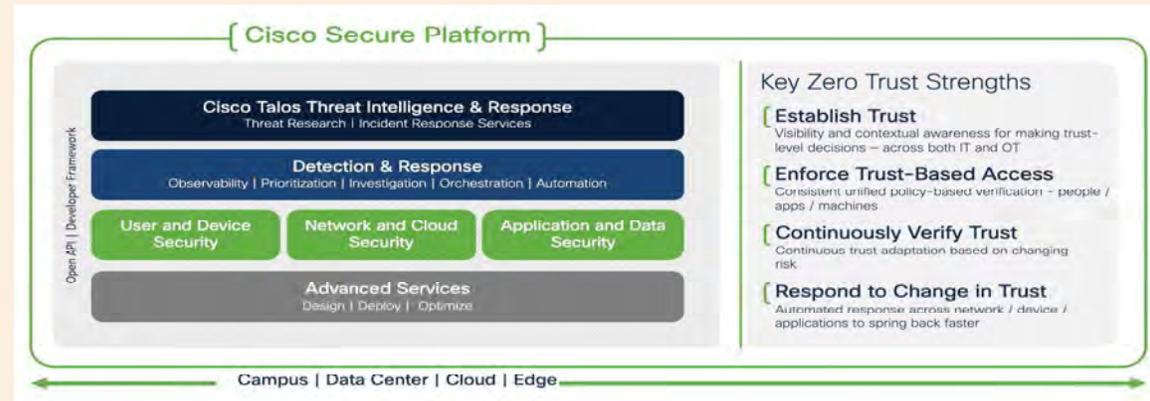
NIST Special Publication 800-207 - Zero Trust Architecture

• The National Institute of Standards and Technology (NIST) develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public.

• NIST defines both Zero Trust and a Zero Trust Architecture as: "Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero Trust Architecture (ZTA) is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies.
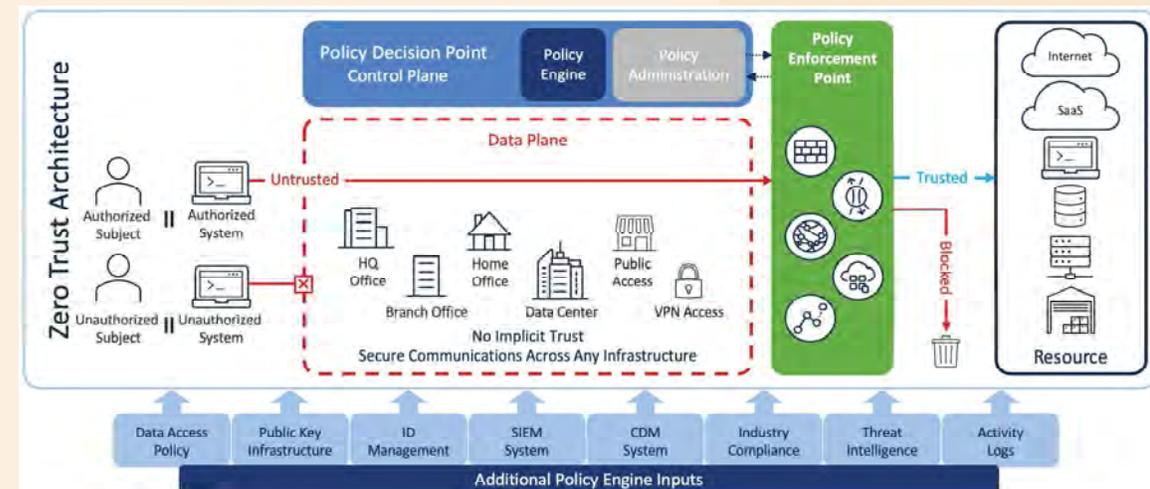
Powering Data Access, Enabling Insight, Serving the Nation

**By Ramon de Guzman, Vice President, Science & Research**

Many of our customers continue to face common mission-critical challenges: modernizing data dissemination infrastructure to meet the rising demands of diverse data consumers, ranging from policymakers and researchers to the general public. With legacy systems limiting scalability, user experience, and real-time data accessibility, the need for a platform capable of ingesting, processing, and securely delivering massive volumes of statistical data is more important than ever . The goal is to unify data from multiple programs—including the into a single, agile platform that could support advanced search, visualization, and API-based integration, all while ensuring compliance with evolving federal cybersecurity mandates.

WHAT WE DID

We provided the operational engine behind Enterprise Data Dissemination Platforms, delivering full-spectrum Operational Support Services. Our team modernized the entire platform stack with a secure, cloud-native architecture—leveraging microservices, containerization, and Infrastructure as Code (IaC) to support dynamic, nationwide data dissemination.

Using a DevSecOps framework, we automate deployments, embed compliance controls, and enable 24/7 operations across development, staging, and production environments. Our Human-Centered Design (HCD) process ensures intuitive, user-driven tools for data exploration, including advanced filtering, mapping, visualizations, and flexible downloads in multiple formats. We also launch robust APIs and a developer portal for seamless third-party integration.

Through Agile and SAFe practices, our cross-functional teams deliver rapid, high-quality releases with automated testing and continuous integration pipelines that minimize defects and accelerate velocity. We introduced the Intelligent Data Dissemination Factory (IDDF)—a scalable framework that powers spatiotemporal analytics, machine learning, and dynamic data product generation.
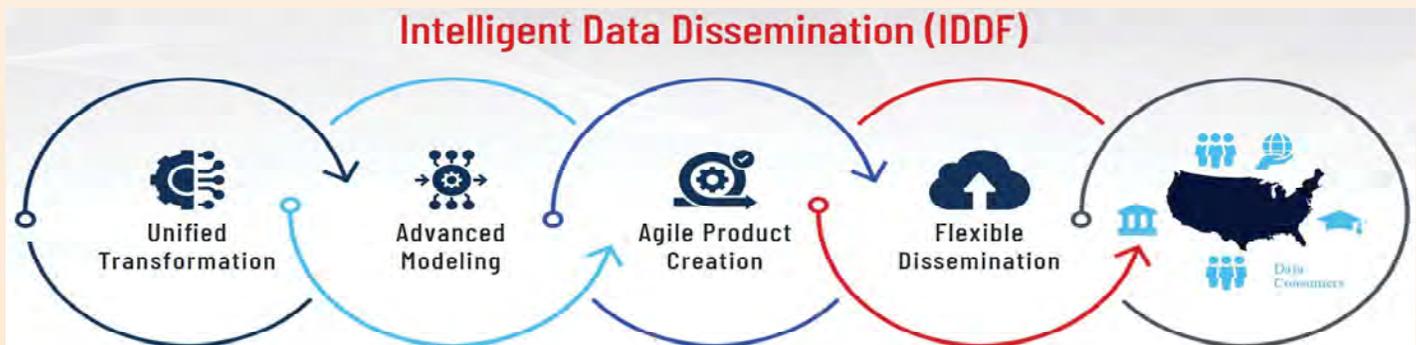
To support real-time performance management, we implement full-stack monitoring, centralized logging, and executive dashboards, giving our customer's leadership team visibility and confidence in decision-making across the platform lifecycle.

OUTCOME

We implemented a seamless solution that provides the following business outcomes to our customer:

- Deliver a fully modernized, scalable, cloud-native dissemination platform.
- Enable 24/7 production operations with automated compliance and security checks.
- Decrease data delivery latency and increase dissemination velocity.
- Integrate 20+ data sources into a unified user experience.
- Expand public access to data through rich visualizations and robust APIs.
- Reduce defect rates through automated testing and early feedback loops.
- Increase stakeholder satisfaction via iterative user-driven design and delivery.
- Support high-profile national data releases with zero downtime.

- ➤ SBA Certified WOSB under NAICS 517111, 517121
- ➤ GWAC and IDIQ Contract Vehicles
  - GSA Alliant 2
  - GSA MAS
  - GSA OASIS Pool 1
  - CIO-SP3 SB/WOSB OTSB
  - DHA MHS GSP
  - DISA Encore III
  - ARMY ITES-3S
  - NAVY Seaport-NxG
  - FAA eFast
  - HHS SPARC
  - NRC GLINDA
  - SEC OneIT
- ➤ Past Performance on Large Contracts
  - DOE ITSS, $1.2B
  - DOT COE, $350M+
  - FAA ATO, $300M+
  - CMS CICDIM, $200M+
  - DOS CA DEDM, $150M+
  - DISA CORENet, $78M
- ➤ CMMI®-DEV V2.0 ML 4 & SAM
- ➤ CMMI®-SVC V2.0 ML 4 & SAM
- ➤ HDI Certified Support Center
- ➤ ISO 20000/27001/9001
- ➤ Approved Accounting System
- ➤ Approved EVM System
- ➤ Approved Purchasing System
- ➤ Approved Cost Estimating System

![TOP WORK PLACES 2014-2025]

"The Navy's presence in this theater is essential, but beyond presence, we must be decisive."

Navy Gold Coast 2025

By Jack Heckerman, Director, Indo-Pacific

As we kick off Navy Gold Coast 2025, meeting with program offices and industry partners, our focus is firmly on the challenges ahead in the Pacific. The Navy's presence in this theater is essential, but beyond presence, we must be decisive.

From the Fleet to Shore operations centers , the fight for warfighter information dominance will define success. We must strengthen cybersecurity, harness machine learning to accelerate decision-making, and expand Foreign Military Sales to ensure our allies and partners are prepared to stand with us.

ActioNet and DecisiveInstincts are proud to stand as a partner in this effort - helping achieve our nation's goals by delivering secure, innovative, and mission-focused solutions for the Indo-Pacific.