Tuesday, April 7, 2026

9 AM EDT
10 MINS

Opening Remarks

Tim Denman
Cybersecurity Learning Director
Warfighting Acquisition University

Ellena Millar
Cybersecurity Professor and Consultant
Warfighting Acquisition University

9:10 AM EDT
40 MINS

The Hazards of a Fully Connected World: Why Cybersecurity Cannot Fail

Nick Espinosa
Chief Security Fanatic
Security Fanatics

9:50 AM EDT
10 MINS

Programming Break

10 AM EDT
25 MINS

Leading to Zero Trust: Principles for a Smooth Journey

Andy Ellis
Legendary CISO
Duha

10:25 AM EDT
25 MINS

Zero Trust for AI Agents

Razi Rais
Senior Product Manager/Architect
Microsoft

As AI agents take on more autonomous roles, securing them requires more than traditional perimeter defenses. This session explores how Zero Trust principles can protect AI driven systems, covering identity verification, access control and behavioral monitoring, so organizations can safely leverage AI without compromising security.

10:50 AM EDT
10 MINS

Programming Break

11 AM EDT
25 MINS

What is Confidential Computing and Why?

Dan Lohrmann
Field Chief Information Security Officer, Public Sector
Presidio

Mark Bower
Chief Strategy Officer
Anjuna

11:25 AM EDT
25 MINS

Why Traditional Networking Fails Agentic AI: Identity-First Connectivity Matters for Zero Trust

Philip Griffiths
Head of Strategic Sales
NetFoundry

11:50 AM EDT
10 MINS

Programming Break

12 PM EDT
50 MINS

The Dual, Evolving Role of AI in Zero Trust

Ken Huang
CEO and Chief AI Officer
DistributedApps.ai

Joshua Woodruff
Founder and CEO
MassiveScale.AI

Chris Kirschke
CISO
Tuskira

Jerry Chapman
Co-Founder & CTO
Numberline Security

Chris Steffen
VP of Research, Information Security, Risk and Compliance Management
Enterprise Management Associates

This panel explores the dual role of Artificial Intelligence in the Zero Trust security model. AI is reshaping the threat landscape by accelerating exploitation, vulnerability discovery, and attack speed, while also strengthening Zero Trust through dynamic access decisions, continuous monitoring, and behavioral analytics. As generative AI, large language models, and agentic systems expand the attack surface across mission systems, cloud environments, and partner networks, organizations must rethink how Zero Trust principles apply across the AI lifecycle.

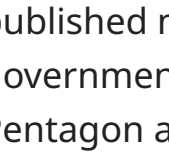
The session will examine how AI can make Zero Trust more adaptive and risk-aware, while Zero Trust provides the identity, policy, and governance foundation needed to scale AI securely in mission environments. Panelists will discuss practical strategies for applying least privilege, explicit verification, and continuous evaluation to protect AI models, data, infrastructure, and operational use - framing AI and Zero Trust as mutually reinforcing disciplines rather than separate initiatives.

12:50 PM EDT
10 MINS

Programming Break

1 PM EDT
25 MINS

Unmanned Attack Surfaces: Agentic AI and Continuous Adversarial Operations



Alissa Valentina Knight
Chief AI Officer, CEO, and Founder
Assail

This session examines how autonomous AI agents are changing the adversarial landscape — chaining reconnaissance, exploitation, and lateral movement without human intervention — and why you need to test their defenses the same way they're being attacked: continuously, intelligently, and at machine speed. Covers API security, AI-driven attack paths targeting payment ecosystems, and the shift from annual pentests to continuous adversarial validation.

Alissa Knight is a two-time successful founder and serves as Founder, CEO, and Chief AI Officer of Assail. With more than 26 years in offensive security, she is widely recognized for her work in adversarial AI systems, autonomous attack simulation, and the application of large-scale AI to offensive security research.

Her work focuses on how intelligent systems discover, exploit, and reason about complex vulnerabilities at machine speed — and how those same systems can be secured. She has published more than 30 vulnerability research reports across financial services, healthcare, and government infrastructure, with findings cited in congressional discussions. She has advised the Pentagon and U.S. Marine Corps on API and application security and is the author of Hacking Connected Cars (Wiley).

1:25 PM EDT
25 MINS

Securing The Agentic Future Requires Zero Trust Principles

Joseph Blankenship
Vice President, Research Director, Security & Risk
Forrester Research

Organizations of all types, including the DoW, are adopting AI at breakneck pace. While AI agents may resemble human users in the types of traditional systems they interact with and the tasks they attempt to carry out, they will do so with greater speed. They may also do so without being deterred by the intentional or incidental security “friction” that ultimately blocks some human behavior. This combination requires the implementation of Zero Trust architecture (ZTA) principles in agentic systems. The principle of least agency and securing intent will be cornerstones of securing agentic systems, and ZTA principles are foundational to those capabilities. Organizations that don’t apply ZTA as part of their AI rollouts run the risk of agents becoming de facto super users as well as backsliding in their broader Zero Trust initiatives. This session will focus on the use of Zero Trust Architecture principles as part of a broader framework to secure, govern, and manage AI agents.

1:50 PM EDT
10 MINS

Programming Break

2 PM EDT
25 MINS

The New Battlefield: Cyber, Drones and Digital Warfare

Mikko Hyppönen
Chief Research Officer
Sensofusion

2:25 PM EDT
25 MINS

Measuring Zero Trust: AI-Orchestrated Purple Teaming and Adversarial Friction

Dan Bradley
Director of Threat-Informed Zero Trust Architecture
Booz Allen Hamilton

2:50 PM EDT
10 MINS

Programming Break

3 PM EDT
25 MINS

Securing Battlespace Against Agentic AI

Ellena Millar
Cybersecurity Professor and Consultant
Warfighting Acquisition University

Agentic AI systems are rapidly transforming the cyber threat landscape by enabling autonomous, scalable attacks with minimal human oversight. This presentation examines two recent real world cases to illustrate how these technologies lower barriers to sophisticated cyber operations. Using a Zero Trust Architecture (ZTA) framework grounded in NIST SP 800-207, the research shows that traditional perimeter defenses are insufficient against AI-enabled threats. Instead, continuous verification, least-privilege access, and microsegmentation significantly reduce attack surfaces and limit adversary movement.

The session highlights why integrating Zero Trust principles is essential for defending mission-critical systems and adapting cybersecurity strategies to the realities of AI-driven threats.

3:25 PM EDT
25 MINS

Bridging the ZT Boundary: OpenTDF as a Critical Enabler for Sovereign, Data-Centric Interoperability

Don Yeske
Senior Solutions Architect, Global Public Sector
Virtru

3:50 PM EDT
10 MINS

Programming Break

4 PM EDT
50 MINS

Speaker Discussion Panel

Daryl Haegley
Technical Director, DAF Cyber Resiliency Office for Control Systems (CROCS)
U.S. Department of the Air Force

Dan Bradley
Director of Threat-Informed Zero Trust Architecture
Booz Allen Hamilton

Philip Griffiths
Head of Strategic Sales
NetFoundry

Mark Bower
Chief Strategy Officer
Anjuna

Karen Uttecht
Technical Staff
MIT Lincoln Laboratory

Featured speakers from across our ZT4 sessions will meet together and answer your questions! Be sure to submit questions in the Q&A box, throughout the day.

4:50 PM EDT
10 MINS

Closing Remarks

Wednesday, April 8, 2026

9 AM EDT
10 MINS

Opening Remarks

Tim Denman
Cybersecurity Learning Director
Warfighting Acquisition University

George Alves
Professor, Enterprise Cybersecurity
Warfighting Acquisition University

9:10 AM EDT
15 MINS

Keynote Speaker

Dr. Brian G. Hermann
Portfolio Acquisition Executive - Cyber
Defense Information Systems Agency

9:25 AM EDT
25 MINS

Zero Trust Implementation Guidelines (ZIGS)

Dr. Shelly Kelly
Chief Operations Officer for Critical Government Systems
National Security Agency

9:50 AM EDT
10 MINS

Programming Break

10 AM EDT
50 MINS

Containment, ZT and the Security Graph - The Path to Anti-Fragility

John Kindervag
Chief Evangelist
Illumio

10:50 AM EDT
10 MINS

Programming Break

11 AM EDT
25 MINS

“AI-First" Warfighting: Re-inventing Existing DoW Workflows to Integrate AI

Dr. Paul Shaw
Independent
Cybersecurity Consultant

“AI-First" Warfighting is a newer DoW core concept. Many of the DoD’s Zero Trust capabilities leverage Artificial Intelligence (AI) and Automation as critical components of their highest maturity levels. AI is critical capability for leverage of newer technologies of advanced ZT defend/deter capabilities and a way to improve critical workflow efficiencies/effectiveness. AI-First Warfighting requires execution on strategic, operational, tactical, and technical levels. Achieving AI-First Warfighting in the DoD’s Zero Trust implementation requires translating security objectives to security engineering implementation. This implementation requires navigating technical considerations and workflow redesign. A public DoW AI use case will be used to examine questions and security engineering considerations for the advanced use of AI capabilities.

11:25 AM EDT
25 MINS

From the Fan Chart to the Fan Room: Making Zero Trust Real in OT

Daryl Haegley
Technical Director, DAF Cyber Resiliency Office for Control Systems (CROCS)
U.S. Department of the Air Force

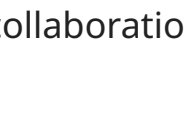
For many, the 105 activities of the DoW Zero Trust for OT Fan Chart feel like a theoretical framework. This session moves past the diagrams and into the operational terrain to show that achieving Zero Trust for Operational Technology is not only possible—it’s already happening.

11:50 AM EDT
10 MINS

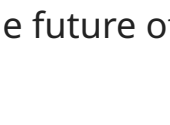
Programming Break

12 PM EDT
50 MINS

Zero Trust for Critical Infrastructure and Operational Technology - Protecting Critical Systems



Chuck Weissenborn
Chief Technology Officer
Dragos Public Sector



Philip Griffiths
Head of Strategic Sales
NetFoundry

Karen Uttecht
Technical Staff
MIT Lincoln Laboratory

Joshua Woodruff
Founder and CEO
MassiveScale.AI

Danielle Jablanski
Cybersecurity Consulting Program Lead, OT Cybersecurity
STV

As cyber threats become increasingly global, the adoption of Zero Trust (ZT) frameworks for Operational Technology is gaining traction across industries and borders. This session explores the international landscape of Zero Trust adoption, highlighting the unique challenges, regulatory considerations, and best practices for organizations worldwide. Join us as experts discuss how different regions and sectors are implementing Zero Trust principles to enhance cybersecurity, protect critical infrastructure, and stay ahead of evolving threats. Learn how international collaboration and diverse perspectives are shaping the future of ZT adoption on a global scale.

12:50 PM EDT
10 MINS

Programming Break

1 PM EDT
25 MINS

Designing for the Unbreakable Future: Zero Trust and Post Quantum Security for the DoW

Renata Spinks-McNeal
CEO
CyberSec International

1:25 PM EDT
25 MINS

OT Integrity Assurance: Detecting Cyber Attacks Inside Industrial Controllers for OT Zero Trust

Robert Johnson
President/CEO
Cimcor, Inc.

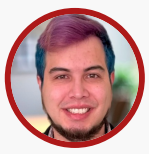
Industrial control systems (ICS) and operational technology (OT) environments face increasing cyber threats with real-world physical consequences, yet most security tools monitor only network traffic and cannot see what occurs inside the controllers that operate industrial processes. This presentation introduces OT Integrity Assurance (OTIA), a new detection approach that combines controller integrity monitoring with behavioral analysis of the physical process. By simultaneously verifying whether PLC logic or configuration has changed and analyzing process behavior through multiple detection algorithms, OTIA can determine not only that a deviation occurred but why it occurred—distinguishing cyber attacks from equipment faults or authorized maintenance. The session also demonstrates how this approach aligns with the Department of Defense operational technology Zero Trust framework by providing the missing inner layer of visibility inside controllers where physical consequences originate.

1:50 PM EDT
10 MINS

Programming Break

2 PM EDT
25 MINS

Featured Speaker



Steve Turner
Cloud Security Architect
Zelis Healthcare

2:25 PM EDT
25 MINS

Zero Trust for Operational Technology

David Voelker
NAVWAR SYSCOM Standardization Officer
U.S. Department of the Navy

This presentation outlines the Department of the Navy's (DON) standardized design process for applying Zero Trust (ZT) security principles to mission-critical Operational Technology (OT) environments. It provides a structured methodology for securing Industrial Control Systems (ICS) and legacy platforms by guiding teams through a process of mission decomposition, system characterization, ZT architecture design, implementation, and validation. The guide serves as a key resource for engineers and program managers, ensuring a consistent and defensible approach to integrating the "never trust, always verify" principle, ultimately producing more resilient and mission-assured OT systems.

2:50 PM EDT
10 MINS

Programming Break

3 PM EDT
25 MINS

AI and Cybersecurity: What's Happening and What's Coming

Phil Venables
Partner
Ballistic Ventures

3:25 PM EDT
25 MINS

Lessons From the Trenches: How and Why for OT Architecture

Bryson Bort
CEO & Founder
SCYTHE

3:50 PM EDT
10 MINS

Programming Break

4 PM EDT
25 MINS

Trust No Signal - Exploiting Digital Energy at Level 0

Paul Coggin
Cyber SME
nou Systems

4:25 PM EDT
25 MINS

Zero Trust for Physics: The Unverified Attack Surface in DefenseAI

John Kruze
CEO
Protocol Company

4:50 PM EDT
10 MINS

Closing Remarks

Thursday, April 9, 2026

6 HRS, 30 MINS

Day #3: Applied Training & International ZT

Day 3 centers on applied training, translating strategy into action through Zero Trust implementation simulations and live demonstrations. Participants will engage with practical scenarios designed to test decision-making, policy alignment, and technical execution in real-world mission environments. Academic partners and representatives from the Warfighting Acquisition University and warfighting communities will showcase hands-on approaches to workforce development, acquisition integration, and operationalizing Zero Trust principles across the enterprise.

In addition to these sessions, Day 3 will feature a dedicated international track, highlighting perspectives from allied partners and global security leaders working to advance Zero Trust principles across multinational environments. Sessions will be dual broadcast, allowing participants to engage with both the applied training program and international discussions throughout the day.

Check back in to see our full agenda!

8:30 AM EDT

5 MINS

Opening Remarks

Tim Denman
Cybersecurity Learning Director
Warfighting Acquisition University

8:35 AM EDT

25 MINS

Cyber Resilience by Design: Establishing Engineering Principles for Mission Assurance in Contested Cyber Environments

Dr. Konrad Wrona
Principal Scientist
NATO

NATO’s adversaries are increasing their cyber activities, quickly adopting new technologies and operating at machine speed. In such a constantly evolving threat environment, perimeter-based security can no longer guarantee that mission-essential functions survive. Although increased enforcement of compliance and accreditation helps confirm that appropriate security controls are in place, it does not ensure operational continuity once a sophisticated actor has already achieved persistent access. The critical question for commanders has shifted from whether systems will be breached to whether the mission continues effectively when they are.
This presentation introduces Cyber Resilience by Design (CRbD), a framework integrating Zero Trust Architecture with the MITRE Cyber Resiliency Engineering Framework to prepare NATO’s communication and information systems for graduated mission survivability under the assumption of compromise. At its core, CRbD is expressed through twelve interdependent engineering principles organized across three categories that must be embedded across the entire system lifecycle.

9 AM EDT

50 MINS

The Mathematics of Cyberwar

Dr. Chase Cunningham
Self
DrZeroTrust

Cyber war is no longer a future possibility—it is a current operational reality, already extracting financial and human costs from the United States at a scale comparable to conventional conflict, just without the cinematic shock of explosions or troop movements. This keynote reframes “cybersecurity incidents” as distributed acts of warfare, showing that cumulative losses from cybercrime and state-aligned operations have run into the trillions of dollars over the past decade, rivaling the cost of major shooting wars, yet remain largely invisible in public discourse and policy. Drawing on data from critical infrastructure, healthcare, and the private sector, the talk demonstrates how “low and slow” campaigns—ransomware against hospitals, supply-chain compromises, IP theft, and systemic fraud—create hidden casualties, degrade national resilience, and shift strategic advantage to adversaries who never have to fire a shot.

Attendees will:

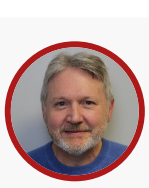
- See a side-by-side comparison of cyber’s economic and human toll versus Vietnam, Iraq, and other U.S. conflicts.
- Understand how the dispersion of events across time, sectors, and jurisdictions prevents a true “war footing” response.
- Learn a practical framework for treating cyber as an operational battlespace—linking doctrine, investment, and Zero Trust implementation to the reality that this war is already underway, and that the current “IT problem” mindset is, in effect, the adversary’s center of gravity.

9:50 AM EDT
10 MINS

Programming Break

10 AM EDT
25 MINS

Zero Trust as Global Policy - How Governments Are Adopting Zero Trust



Sean Connelly
Executive Director, Global Zero Trust Strategy and Policy
Zscaler

Zero Trust has moved beyond U.S. federal policy and is now shaping cybersecurity strategy at the national, allied, and sub-national level. This session traces the arc from the SolarWinds-driven policy response — EO 14028, OMB M-22-09, NIST SP 800-207, and the CISA Zero Trust Maturity Model — to active adoption by a growing number of governments and jurisdictions worldwide. Drawing on his experience as co-author of both NIST SP 800-207 and the CISA ZTMM, the speaker examines the common architecture language, policy structures, and maturity frameworks that are converging across programs. The session concludes with practical observations on what distinguishes programs gaining ground from those still treating Zero Trust as a compliance exercise.

10 AM EDT
25 MINS

Tailoring Security and Zero Trust Principles to Weapon System Environments

Tim Morrow
Situational Awareness Technical Manager, CERT Division
Carnegie Mellon University I Software Engineering Institute

Department of War (DoW) stakeholders need guidance on how to tailor and adapt a zero-trust strategy to weapon system platforms. Carnegie Mellon University conducted a study that analyzed the applicability of nine foundational security and zero trust principles to weapon system environments. These principles define a framework for making security decisions, implementing security controls, and enabling mission assurance through effective risk management.

10:25 AM EDT
25 MINS

Advancing Proactive Cyber Defense: Integrating Human and Machine Intelligence for Modern Cybersecurity

Dr. Calvin Nobles
Portfolio Vice President and Dean, School of Cybersecurity, and Information Technology
University of Maryland Global Campus

This presentation positions threat hunting as a central pillar of proactive cyber defense and examines how it can be strengthened through the integration of Zero Trust architecture, Security Operations Center (SOC) operations, artificial intelligence, and human factors engineering. Rather than waiting for alerts or confirmed compromise, the presentation emphasizes the value of actively searching for hidden adversary behavior, weak signals, and emerging attack patterns before they escalate into significant incidents. The presentation argues that threat hunting is most effective when supported by Zero Trust principles that reduce implicit trust, continuous monitoring practices within the SOC, and AI-enabled analytics that enhance speed, pattern recognition, and anomaly detection. At the same time, it underscores that successful threat hunting remains deeply dependent on human judgment, contextual reasoning, and analyst decision-making. For this reason, human factors engineering is presented as essential to reducing cognitive overload, mitigating fatigue, and designing tools and workflows that support better investigative performance. Overall, the presentation advances a unified model of cyber defense in which threat hunting serves as the operational centerpiece connecting technology, intelligence, and human expertise. This approach moves organizations beyond reactive security and toward a more adaptive, resilient, and intelligence-driven defense posture capable of countering increasingly complex cyber threats.

10:25 AM EDT
25 MINS

The Zero Trust Maturity Myth

Jennifer Minella
Advisory CISO
Carolina Advanced Digital, Inc.

Zero Trust isn’t a finish line -- it’s a moving target. In this session, we cut through the hype around maturity models and break down what Zero Trust actually looks like in practice across users, workloads, and networks. You’ll learn how to structure a program around real protect surfaces, evolving business needs, and continuous feedback loops—so progress is measured by adaptability, not a misleading sense of “done.”

10:50 AM EDT
10 MINS

Programming Break

11 AM EDT
15 MINS

Securing Critical Infrastructure with Zero Trust: CCZT Training Overview

Anna Campbell Mckee
Director of Training Programs
Cloud Security Alliance

As organizations work to protect critical infrastructure with Zero Trust architectures, there is a growing need for practitioners who can translate these principles into operational controls in complex environments. The Cloud Security Alliance's (CSA) CCZT program provides vendor-neutral training aligned to NIST and CISA guidance, emphasizing identity, device posture, and contextual signals for continuous authorization. This overview sets the foundation for a hands-on demonstration of how these controls are applied to secure access to sensitive, mission-critical resources.

11 AM EDT
20 MINS

Why OT Needs Zero Trust More Than IT: 10 Years of Insights

Lieuwe Jan Koning
CEO
On2IT

Rob Maas
Field Chief Technology Officer
On2IT

11:15 AM EDT
35 MINS

Zero Trust in Practice: CCZT Hands-On Demonstration

Jason Garbis
Founder and CEO
Numberline Security

As federal agencies accelerate adoption of Zero Trust architectures, workforce readiness has become one of the most critical challenges. This session uses an interactive exercise to illustrate how Zero Trust concepts are applied in practice. Attendees will see how identity, device posture, and contextual signals can be used to dynamically authorize access to protected resources, providing a practical view of how Zero Trust principles translate into real-world implementation.

It will also provide an overview of the Certificate of Competence in Zero Trust (CCZT) training program developed by the Cloud Security Alliance (CSA). The CCZT is a vendor-neutral program designed to help security professionals understand foundational Zero Trust concepts, architecture models, planning strategies, and implementation considerations, drawing on widely recognized guidance and frameworks from organizations such as NIST, the U.S. Department of Defense, and CISA.

Presenters Jason Garbis, co-author of Zero Trust Security: An Enterprise Guide, and Anna Campbell McKee, Director of Training Programs at Cloud Security Alliance, will discuss how structured training can strengthen cybersecurity workforce capability and help organizations transition from perimeter-based security models to modern Zero Trust architectures.

11:25 AM EDT
25 MINS

Securing Global Development: The World Bank Group's Pivot to Zero Trust

Remy Faures
Manager - Global Head Information Security
World Bank

As digital transformation becomes a cornerstone of global development, the World Bank Group (WBG) is redefining security to protect its mission of ending extreme poverty and promoting shared prosperity. This session explores the WBG's multi-year journey in implementing a Zero Trust Architecture (ZTA), a strategic shift catalyzed by the ransomware epidemic and the transformation induces by the cloud adoption. This presentation details how identity has emerged as the "nervous system" and new control plane of the organization, requiring robust governance and a focus on seamless user experiences, such as the migration to passwordless authentication. Drawing on lessons from the U.S. Federal government's leadership—including the CISA Maturity Model—we will discuss how these frameworks provide a pragmatic blueprint for building cyber resilience in complex, global environments. We will further examine how the Zero Trust approach can scale to support the AI transformation.

11:50 AM EDT
10 MINS

Programming Break

12 PM EDT
25 MINS

Segmenting OT Networks: Reducing Risk Without Impacting Reliability

Larry Grate
OT Cyber SME
Aleta Technologies, Inc.

This presentation provides an overview of network segmentation as a foundational security control within Operational Technology (OT) environments. It outlines key architectural principles, highlights common vulnerabilities in flat network designs, and emphasizes segmentation's role in reducing risk, containing faults, and enhancing the resilience of critical OT systems.

12 PM EDT
50 MINS

ZT Program Management Panel

Jason Garbis
Founder and CEO
Numberline Security

Remy Faures
Manager - Global Head Information Security
World Bank

Daryl Haegley
Technical Director, DAF Cyber Resiliency Office for Control Systems (CROCS)
U.S. Department of the Air Force

Sean Connelly
Executive Director, Global Zero Trust Strategy and Policy
Zscaler

Danielle Jablanski
Cybersecurity Consulting Program Lead, OT Cybersecurity
STV

As cyber threats become increasingly global, the adoption of Zero Trust (ZT) frameworks is gaining traction across industries and borders. This session explores the international landscape of Zero Trust adoption, highlighting the unique challenges, regulatory considerations, and best practices for organizations worldwide. Join us as experts discuss how different regions and sectors are implementing Zero Trust principles to enhance cybersecurity, protect critical infrastructure, and stay ahead of evolving threats. Learn how international collaboration and diverse perspectives are shaping the future of ZT adoption on a global scale.

12:25 PM EDT
25 MINS

How to visualize and microsegment modern networks

Gary Barlet
Public Sector Chief Technology Officer
Illumio

Modern threats are evolving faster than humans can respond. Learn how Zero Trust tools providing visualization and label-based segmentation can help defend against these growing threats. See firsthand how threats can be neutralized across even the largest, most complex environments.

12:50 PM EDT
10 MINS

Programming Break

1 PM EDT

50 MINS

Resilient Zero Trust: From Single Points of Failure to Adaptive Defense

Francesco Chiarini
Founder and Lead Instructor Cyber Resilience Academy
ISSA.org Cyber Resilience Special Interest Group

Alex Sharpe
Board Member
Sharpe LLC

Denis Nwanshi
CEO
NetraScale

Dr. Georgiana “George” Shea
Chief Technologist of Transformative Innovation Lab
Foundation for Defense of Democracies

Steve Pitcher
Former Senior Cyber Survivability Analyst
Joint Staff (Ret.)

Zero Trust plays a foundational role in achieving cyber resilience by shifting the focus from a perimeter-based defense to an identity-centric model that assumes "breaches happen". While traditional security often creates brittle environments where a single failure can lead to total collapse, a resilient Zero Trust architecture is designed to maintain security posture and business continuity even when specific components fail or third parties are disrupted.

The integration of Zero Trust and resilience involves several key strategies:

- **Eliminating (or reducing) Single Points of Failure (SPOF)**. A single disruption inside of an enterprise can cause a major incident. In today’s highly connected enterprise, we also need to be mindful of the Single Points of Failure that exist outside of the enterprise, like Cloud Service Providers (CSP) and within our supply chains.
- **Limiting the blast radius to thwart contagion and cascading failures.** We have all seen how a single disruption can rapidly move across an enterprise bringing the entire business to its knees. In today’s highly interconnected world, we also need to be mindful of third-party disruptions entering our enterprise.
- **Adaptive Defense and Graceful Degradation.** By accepting that incidents will happen allows us to prepare for the day, so we can operate in an impaired state until we are fully restored. Shifting workloads out of region, falling back to manual processes, throttling services, and prioritizing constituents are considered.
- **Business Priorities.** Nobody has unlimited resources. We prioritize based on the priorities of the business. The Business Impact Analysis (BIA) gains increased importance.
- **Design Resilience in from the beginning, Test, Continuously Monitor.** Ultimately, Zero Trust serves as the foundation for a resilient enterprise where the organization not only survives security incidents but also learns from them to improve its long-term operational effectiveness. Zero Trust Architectures, Site Reliability Engineering (SRE), Security By Design, chaos engineering and chaos testing are key to the prevention and the early detection of incidents to foster recovery.

1 PM EDT
25 MINS

Zero Trust: Training Capabilities

Lee Aguilar
Cloud Solutions Architect
Microsoft

This session provides a practical, training-focused introduction to Zero Trust, mapping core principles—verify explicitly, least privilege, and assume breach—to industry certifications such as AZ-900 and SC-200. Attendees explore hands-on learning paths, applied skills, and structured assessments, including the DoD Zero Trust Workbook, to support skill validation, posture assessment, and alignment with Department of Defense Zero Trust expectations.

1:25 PM EDT
25 MINS

Integrity Assurance for Zero Trust: From Detection to Deterministic Defense

Mark Allers
Vice President, Business Development
Cimcor, Inc.

Traditional cybersecurity tools rely heavily on probabilistic detection techniques that identify suspicious behavior after an attack has already begun. Integrity Assurance introduces a deterministic approach to cybersecurity by continuously validating the integrity of critical system components and enforcing trusted baselines. When unauthorized changes occur, organizations can immediately detect, alert, and automatically remediate those changes, reducing adversary dwell time and preventing attackers from establishing persistence. For this reason, it is called out as Tenet #5 in NIST 800-207.

In the context of DoW's Zero Trust Strategy, integrity validation and enforcement contribute directly to over two dozen Zero Trust Target Level Activities within the 91 activity framework, particularly those associated with system configuration/change management, workload protection, and automated security response and remediation. By ensuring that devices and workloads remain in their approved and trusted state, Integrity Assurance strengthens Zero Trust architectures and enforces the "never trust, always verify" principle. This presentation will demonstrate how deterministic integrity enforcement enables organizations to move beyond detection toward a more resilient, self-correcting cybersecurity posture.

1:50 PM EDT
10 MINS

Programming Break

2 PM EDT
50 MINS

Zero Trust Without Borders: Securing Allies and the Global Defense Industrial Base

Derek Doerr
US Federal Zero Trust Lead, WWPS
AWS

Jordan Burris
Head of Public Sector
Socure

Jim Smid
DoD Intel SA
Palo Alto Networks

Tom Suder
President & Head of AI Transformation
ATARC

In a dynamic, discussion-driven forum, these experts will explore the latest developments, real-world challenges and best practices for extending Zero Trust principles across NATO alliances, international partnerships and defense industrial base operations overseas, all within an increasingly complex global threat environment.

2 PM EDT
25 MINS

BitW Shield: Zero Trust for Legacy Operational Technology

Thomas Jewkes
Assistant Professor of Practice, College of Information Science
University of Arizona

Mr. Thomas Jewkes will explain zero trust with real-world examples rather than abstract concepts, highlighting how people already use zero trust in their daily lives. The presentation will address the challenges of IT/OT and identify where threats can breach the OT network. It will conclude with a BitW demo, showing how it reduces remote access and eliminates a key attack vector.

2:25 PM EDT
25 MINS

Agentic AI Security: Threats, Evaluation, and Defenses

Dr. Daniel Takabi
Director, School of Cybersecurity
Batten Endowed Chair in Cybersecurity &Director, Coastal Virginia Center for Cyber Innovation
Old Dominion University

2:50 PM EDT
25 MINS

When AI Breaks Security: Why Zero Trust Is No Longer Optional

Rich Mogull
Chief Analyst
Cloud Security Alliance

AI isn't just changing the threat landscape, it's breaking fundamental assumptions we've built enterprise security on for decades. In my "Core Collapse" research, I showed how advanced AI models constrain the attacker's problem space while expanding the defender's to near-infinity, and the math only gets worse as models keep advancing. AI-accelerated exploit development already outpaces our response cycles, and traditional defenses like patching windows and signature detection can't keep up. This doesn't mean the end, and we don't even need new technologies, we just need to go back to our preventative fundamentals. Zero Trust creates architectural resilienceand defense in depth at exactly the moment AI makes single-point failures so problematic. In this session I'll cut through the hype and focus on practical implementation: which Zero Trust principles matter most right now, how to prioritize when you have limited resources, and why organizations that build these foundations today won't find themselves scrambling when the next wave of autonomous AI capabilities hits.

2:50 PM EDT
10 MINS

Programming Break

3 PM EDT
25 MINS

Addressing SOC Log Fatigue ... While Operationalizing Zero Trust

Jerry Derrick
Senior Solutions Architect
Elastic

As mandates for Zero Trust adoption accelerate, so does the volume of data, alerts, and operational complexity that face front-line defenders. This session looks at Zero Trust through the lens of SOC analyst fatigue, exploring how continuous verification can unintentionally overwhelm the very teams responsible for defending the mission. Attendees will hear how better visibility, normalized data, behavioral baselines, and AI-assisted analysis can help reduce noise, improve response, and make Zero Trust more effective in practice.

3:25 PM EDT
25 MINS

Making Zero Trust Actionable: How Integration and AI Turn Signals into Decisions

Jim Smid
DoD Intel SA
Palo Alto Networks

Move your Zero Trust strategy from compliance and checkboxes to outcomes and actionable intelligence. We examine real-world examples and how integrating data, automation and AI transform the platform into measurable results that safeguard the mission. Every pillar of zero trust must work together as a cohesive ecosystem, feeding advanced algorithms to recognize and react to threats.

3:50 PM EDT
25 MINS

Securing the Agentic Enterprise

Dr. Heath Gross
Professor of Cybersecurity
Warfighting Acquisition University

A definitive guide to implementing Zero Trust architecture for autonomous AI, preserving data privacy, and mitigating next-generation cyber threats.

4:15 PM EDT
15 MINS

DoW Zero Trust Training Plan – FY26 and Beyond/ Closing Remarks

George Alves
Professor, Enterprise Cybersecurity
Warfighting Acquisition University

This presentation outlines a workforce-aligned approach to institutionalizing Zero Trust as both a security framework and cultural shift across the Department of the War. It integrates Zero Trust training from Academia, Commercial and WarU offerings into DoW components, workforce requirements, and qualification standards aligned with DoDD 8140 and the Defense Cyber Workforce Framework. The plan proposes a tiered Zero Trust Qualification Pathway and a comprehensive training ecosystem spanning awareness courses, practitioner workshops, cyber training ranges, and advanced system-specific exercises. Together, these efforts enable scalable, role-based adoption of Zero Trust across IT, operational technology, and the acquisition lifecycle.