

Zero Trust: Where it's expanding next



SITREP

To protect Pentagon information technology systems, the DoD CIO Zero Trust Portfolio Management Office has developed a comprehensive Zero Trust strategy that defines 152 ZT activities and identifies a minimum of 91 target-level goals that must be achieved across the entirety of the DoD by the end of fiscal year 2027. The goal is 100-percent cyber protection of its IT infrastructure at the target level set by the DoD CIO office.

To support this, the office has secured funding and resources from DoD leadership to drive proof-of-concept efforts and implementations across the department by the deadline. Collaboration with military services, agencies, and industry is ongoing to identify and assess various solutions that meet target and advanced levels for Zero Trust. These architectures involve integrating dozens of cybersecurity vendor products into cohesive ZT packages under the direction of main systems integrators that are sold as complete turnkey systems.

So far in this effort, the DoD CIO has assessed and affirmed several Zero Trust architectures that meet target levels plus another 61 advanced level requirements.

These are the Defense Information Systems Agency's Thunderdome, the US Navy's Flank Speed, and Dell Technologies' Fort Zero.

A key goal of the DoD's Zero Trust strategy is to prevent adversary exploitation of DoD data and systems, even if the adversary has already penetrated the network, through measures like micro-segmentation and continuous behavioral monitoring that focus primarily on users and devices. With threats ever increasing, however, the DoD CIO office is now expanding Zero Trust principles from IT systems to operational technology (OT) like industrial control systems and Internet of Things devices, along with weapon systems.

In this eBRIEF, we will discuss the present status of DoD Zero Trust with Randy Resnick, director of the DoD CIO's Zero Trust Portfolio Management Office, what DISA and the Navy did to achieve target-level ZT, and how Zero Trust can be expanded from IT to OT.

— *Barry Rosenberg*
Technology & Special Projects Editor, Breaking Defense

U.S. Air Force Senior Airman Marion Contreras, a cyber systems operator assigned to the 378th Expeditionary Communications Squadron, establishes a satellite network system during Exercise Agile Spartan 23-4, within the U.S. Central Command area of responsibility, March 4, 2023. (U.S. Air Force photo by Tech. Sgt. Daniel Asselta)



ON THE COVER: U.S. Air Force Senior Airman Jeremy Saludo, 18th Communications Squadron node site coordinator, lifts floorboards to access wires at Kadena Air Base, Japan, Sept. 8, 2023. The 18th CS airmen are responsible for the upkeep and protection of the base's cyber infrastructure. (U.S. Air Force photo by Airman 1st Class Catherine Daniel)

You couldn't buy a box of Zero Trust a few years ago but now something akin to that is ready

When the DoD CIO office began its Zero Trust journey earlier this decade with the goal of stopping an adversary's desire to exploit DoD data or to even touch the data, it used as its template the Mitre ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework released in 2013. The ATT&CK matrix classified and described cyberattacks and intrusions across 14 pillars and 245 adversarial activities.



Randy Resnick, director of the DoD CIO's Zero Trust Portfolio Management Office, in a 2022 image. (DoD photo)

"What we did is reverse engineer the Mitre attack framework, which was the best representation of adversary tactics, techniques, and procedures," Randy Resnick, director of the DoD CIO's Zero Trust Portfolio Management Office, explained to Breaking Defense.

"If we were to stop the ability of an adversary to exploit DoD data, we essentially had to address mitigations of all the cells in the Mitre attack framework. That had never been attempted nor even contemplated."

The result is the 152 activities in the DoD CIO Zero Trust strategy playbook that everyone is now working from, with each one of those activities intended to address or mitigate one or more of the cells within the Mitre attack framework. Said Resnick: "Anything less than not being able to stop the adversary still allows the adversary to get in at some level and potentially manipulate or steal data. We've spent tens of billions of dollars easily over the last 30 years in traditional cybersecurity that has still not been able to prevent adversary exploitation. It had to be an all or nothing strategy because we were trying to fix what legacy cybersecurity couldn't do, no matter how much money you threw at the problem."

Resnick emphasized that the strategy is not a checkbox and the DoD CIO is not telling military services or industry how to address the ZT targets. What the office did quickly realize, though, was that no single company could deliver target-level ZT on its own.

For example, DISA's Thunderdome and Dell's Fort Zero integrated approximately 25-35 different cybersecurity capabilities, according to Resnick. Visible to the naked eye may be only a couple racks of equipment, but inside are several dozen virtualized cyber systems.

"From a user's perspective, they're buying a Thunderdome, they're buying a Fort Zero, but under the hood they're buying 35 products," said Resnick, speaking generally. "They no longer have to integrate together on their own, which was what the DoD was doing prior to 2022. We were integrating various cybersecurity products thinking we knew what we were doing and quite frankly, we did a poor job over the last 30 years because we just don't know how to integrate products together."

"We were doing essentially the IKEA model of building cybersecurity. That's not our ball of wax. We have to fight wars and achieve military objectives for cybersecurity. Attacks are so complex from our adversaries now and they're coming at velocities unheard of 10 years ago that we need to not only keep up and address what's happening but we need to exceed it."

That means a combination of stopping the adversary at the front door, which is what Zero Trust is intended to do, but then also ensure that if there is a breach there are sensors, visibility, and analytics that identify them.

Attendees at AFCEA TechNet conferences in Baltimore in the 2019-2020 timeframe may remember when Zero Trust first came on the scene and vendors across the exhibitor floor were all touting a "box of Zero Trust." Such a thing never existed, but now there's a close approximation – even if it's more akin to a nesting doll.

"At the beginning, even in our own briefings, we made statements to the audience that you can't buy Zero Trust; we meant it in the sense that no amount of money is going to buy you out of this problem," said Resnick, explaining that the



Servicemembers work on computers during an Innovative Readiness Training event May 8, 2024, in Corpus Christ, Texas. The 10-day event took place at the Nueces County courthouse where 29 members of the Air Force reserve, active-duty Air Force and Space Force Guardians performed a vulnerability assessment of the county's cybersecurity. (U.S. Air Force photo by Master Sgt. Rachelle Morris)

original idea was that many individual companies would lash together their products without necessarily needing a lead systems integrator.

“We were unexpectedly surprised in a positive way when we saw that bigger companies saw an advantage in integrating other products together in a win-win situation between the integrator and the vendors involved. They’re still selling to the government, but they’re selling it through an integrator, which is exactly along the business lines that companies are familiar with doing.”

Flank Speed, Thunderdome, Fort Zero

These three programs are the first and only Zero Trust implementations that have met all target-level ZT goals and most if not all advanced activities, according to the DoD CIO office. The following is a brief overview of each, all built around on-premise cloud capabilities.

Flank Speed & Hyperion

The Navy’s Flank Speed ZT implementation is a cloud service in development since 2021 by the Navy Program Executive Office for Digital and Enterprise Services (PEO Digital) and US Fleet Cyber Command. Operations are managed by Navy Network Warfare Command, with cybersecurity responsibilities falling to Navy Cyber Defense Operations Command.

“Aligning the Department of Navy with Zero Trust principles was born out of a sense of urgency to deliver a secure collaboration and communications platform that would support the massive telework demand triggered by COVID,” said Department of the Navy CIO Jane Rathbun, before leaving the post in August. “We could have tried to modernize the existing collaboration platform, but given the sense of urgency, we moved ahead with a greenfield approach allowing us to architect Zero Trust activities into every aspect of the ecosystem. The implementation was a real change in how we deliver and operate capability, tightly partnering between the resource, requirements, acquisition, and cyber operator communities.”

Earlier this year, Flank Speed and the Marine Corps’ Hyperion, the name for each service’s unclassified Microsoft 365 cloud environment, were designated as DON Enterprise IT Services for messaging and productivity. It’s the first time in the history of the two services that Navy and Marine

Corps information technology systems have been brought together for any enterprise-wide IT solutions.

“Enterprise IT Service designation solidifies Flank Speed and Hyperion as critical Zero Trust enablers of the DON’s digital workplace,” said PEO Digital Executive Director Jeffrey Proudfoot. “Flank Speed and Hyperion ensure that our Navy and Marine Corps personnel can perform their warfighting mission using cloud-enabled platforms from shore to ship, in flight and at the tactical edge. This unity strengthens DON’s ability to execute missions effectively while maintaining continuously compliant security standards.”



New York Air National Guard 107th Attack Wing space systems operators work through a space scenario during CRUZEX CYBER at Natal Air Force Base, Brazil, Nov. 8, 2024. The training aims to fortify the resilience of critical military infrastructure and strengthen the strategic partnerships within the region. (U.S. Air Force photo by Staff Sgt. Madeline Herzog)

Thunderdome

The Thunderdome ZT architecture is now fully fielded across DISA’s enterprise on both classified and unclassified networks. It’s also being deployed to mission partners at the strategic, operational, and tactical levels. This includes the fourth estate, which are those DoD agencies and departments not directly part of the individual military services or intelligence agencies.

Thunderdome consists of a Hyper Scaled Impact Level 5, Secure Access Service Edge (SASE) platform. It integrates

with each organization’s identity and access management systems, and access controls are available for remote users in CONUS and OCONUS.

“Thunderdome enforces Zero Trust policies for on premise users [and] provides SD-WAN, CESS (Customer Edge Security Stack), IDS/IPS (Intrusion Prevention System/Intrusion Detection System) service to enforce conditional access by integrating with identity services,” according to a DISA overview prepared by Christopher Pymm, presently DISA’s PEO Cyber Directorate deputy and former DISA portfolio manager for Thunderdome.

At the recent Technet Cyber 2025 conference, DISA Deputy Director Christopher Barnhurst noted: “The key point in all of that is we went from a concept on a whiteboard, quite literally, to articulating that concept, that vision, to this forum, to then partnering with a number of industry partners in the room here,” as reported by AFCEA, the show’s sponsor. “Dozens of products that are integrated into that design [were provided by our industry partners], and that is now real, and it’s real two years ahead of when the DoD chief information officer said it has to be real for the department.”



Cyber Shield participants compete in the annual “NetWars” games during the Cyber Shield training event held at the Virginia National Guard State Military Reservation in Virginia Beach on June 7th, 2024. SANS NetWars focuses on the practical application and assessment of hands-on cybersecurity training. Cyber Shield is the longest-running and largest Department of Defense cyber exercise that is composed of approximately 900 National Guard and Army Reserve Soldiers, Airmen, civilian cyber professionals, and international partners from across the globe. (North Carolina National Guard photo by Staff Sgt. Hannah Tarkelly).

Project Fort Zero

Dell’s Project Fort Zero is the latest to achieve compliance with the DoD CIO’s target levels as an on-premises private cloud.

“By bringing together an ecosystem of partners and taking on the technology integration of this complex architecture, Dell has laid the groundwork for a turnkey zero trust solution that global organizations can look forward to leveraging the moment it’s deployed,” said Herb Kelsey, industry chief technology officer for government at Dell Technologies. Dell’s Fort Zero architecture also addresses all targets within the seven Zero Trust pillars outlined by the DoD CIO office: user trust, device trust, data trust, application and workload, network and environment, visibility and analytics, automation and orchestration. An example of a device trust target is inclusion of “device help tool gap analysis.” An advanced level capability for device trust is fully managed bring-your-own-device and Internet of Things support.

Zero Trust for operational technology

With three fully compliant ZT implementations now approved for use within the Defense Department, Resnick foresees that those and others will soon find their way to federal agencies, the intelligence community, Five Eyes partners, NATO, and friendly foreign governments.

“The marketplace for Zero Trust is off the charts and everybody is asking for Zero Trust now because they know the crazy

objective of being able to prevent or stop the adversary’s penetration to exploit data has been demonstrated. That’s what they want because they’re under the same attacks and threats that we are faced with ourselves. They’re looking at the successes and are seriously now educating themselves as to which combinations they want to buy to secure 100 percent of their infrastructure.”

The next challenge for the DoD CIO is to bring the ZT strategy created for information technology to operational technology (OT) such as factory floor robots that build cars and others that crawl the floors and climb the shelves of Amazon warehouses. OT is also widely embedded in critical infrastructure such as water and energy in the form of switches, valves, sensors, and monitoring equipment.

The goal of a cyber attack on OT is to use it as a jump-off point to gain entry into an organization’s IT operations that can eventually lead to an adversary accessing proprietary data and intellectual property. For example, a thermostat on the wall is an OT attack vector if it has a WiFi chip that connects to an IT system.

“Colonial Pipeline is a perfect public example of what happened by essentially taking over the OT system of Colonial Pipeline for the purposes of ransomware,” said Resnick. “For a few days, it created minor panic in the population that thought they were going to run out of fuel.

That’s a national security issue. That’s a homeland security issue. There is a large connection between the protection of the homeland and national security.

“Almost every attack on the US in some fashion becomes a point of concern within the Department of Defense and/or the Intelligence Community depending on the severity and [what] I’ll call the blast radius of the attack. When it comes to OT systems, of course the Department of Defense needs to protect those systems ideally in a ZT way.”

There’s no MITRE attack framework or equivalency for securing OT, but the DoD CIO office is adapting its information technology ZT framework of target levels/advanced activities and converting it into OT language. The DoD CIO had planned to release a fan chart for what ZT for OT would look like by defining target and advanced goals, according to Resnick, with a date for compliance to be set, but that release has been delayed due to the government shutdown in fourth-quarter 2025.

Same for the prospective release date for the DoD CIO’s fan chart for the Internet of Things—particularly wireless devices used by warfighters that connect through Bluetooth or WiFi. The DoD CIO office also had planned to release the 2.0 version of Zero Trust for IT in the latter half of 2026.

STOPPING FILE-BASED THREATS AS A VECTOR FOR CYBERATTACKS IN THE ZERO TRUST ERA



Kelly Davis is a Senior Solutions Architect and DevOps Engineer at Glasswall.

File-based threats remain a primary vector for cyberattacks, and in Zero Trust architectures, treating data and files as untrusted is as important as verifying users and devices. As a result, across the U.S. Government, file sanitization is now required by national-level directives to protect critical data transfers across different classification boundaries.

Helping address these requirements, Glasswall's Content Disarm and Reconstruction (CDR) technology is a mandated National Security Agency's (NSA) "Raise the Bar" (RTB) solution. It offers a proactive, Zero Trust approach to file sanitization that fundamentally differs from traditional detection-based methods like antivirus and sandboxing solutions.

Instead of searching for known malicious signatures, Glasswall treats all files as untrusted. Each is deconstructed, cleansed of potentially harmful elements, and rebuilt to its original manufacturer's "known good" specification before being released to users.

To learn more, Breaking Defense talked with Kelly Davis, senior solutions architect and DevOps engineer at Glasswall, to understand the strategic importance of file-based threat protection in national security environments and how CDR is being operationalized across government and defence use cases.

Breaking Defense: What types of files are most vulnerable?

Davis: Threat actors typically target the most commonly used and trusted file types because they offer the widest possible attack surface. These include PDFs, Microsoft Office documents (Word, Excel, PowerPoint), and various image file formats.

The vulnerability of these files stems not just from their everyday use but also from their inherent complexity. Modern file formats can contain a multitude of elements beyond the visible content, such as embedded objects, scripts, macros in Office files, or layers and interactive features in PDFs. These complex structures provide numerous hiding places for malicious code that can evade traditional detection-based security systems.

A big part of the security challenge is that these file types are also integral to mission-critical documentation, intelligence reports, operational plans, technical manuals, and even software updates delivered to warfighters in forward environments.

Maintaining the integrity of these documents as they traverse various networks and echelons is paramount to operational success and security.

How does your Content Disarm and Reconstruction (CDR) technology work?

Instead of attempting to detect and identify malicious content within a file, Glasswall CDR process treats all incoming files as untrusted by default. To ensure they are safe, we apply a patented four-step file protection process: Inspect, Rebuild, Clean, and Deliver.

Inspect: First, the file is deconstructed into its fundamental components. Its underlying structure is meticulously validated against the original manufacturer's "known good" specification for that file type. This means we understand what a truly safe and correctly structured Word document or PDF should look like at its most granular level.

Rebuild: During this stage, any structural deviations, malformations, or unknown elements within the file that don't conform to the official specification are repaired or brought into conformance.

Clean: Concurrently, any potentially risky active content, such as macros, embedded scripts, or other elements that could carry a malicious payload, is removed or neutralized.

Deliver: Finally, the file is reconstructed. The result is a new, safe version of the file that is visually identical and fully functional, but now free of any hidden threats.

This approach eliminates the need for detection signatures, making Glasswall CDR potent against zero-day exploits and sophisticated malware that traditional antivirus tools and sandboxing techniques often miss. Traditional methods are reactive, and they need to have seen a threat to recognize it. We proactively ensure the file is built correctly and safely from the start. This ability to deliver both robust security and full usability is a major advantage, especially in environments where both are non-negotiable.

Recent Navy guidance emphasizes extending Zero Trust principles to all assets and environments, further highlighting the importance of comprehensive data protection. Tell us about this.

The recent moves by the Department of the Navy represent a significant development in their cybersecurity posture. We know target-level Zero Trust is what they're looking to achieve, but one key point from the Navy blueprint is that they're pushing to infuse more Zero Trust into operational technologies.

They are aggressively pushing to achieve target-level Zero Trust capabilities by Fiscal Year 2027. This is a clear signal that the never trust, always verify mantra now applies, extending far beyond traditional IT networks and user access.

The idea is that data itself must be protected regardless of where it resides or how it's accessed, and the goal is to take and review hardware, software, and cybersecurity baselines and recompose how they are structured.

The Navy is also developing new standards to bring weapon systems, control systems, and other mission equipment items into this Zero Trust framework. This obviously increases the scope of assets requiring enhanced security measures by not only looking at the network, traffic, user logins, and authorizations, but also by applying Zero Trust by default for everything, which is a very positive step.

Final thoughts?

Zero Trust is a journey, and the one common theme across the military is that they want to get back to basics and clearly define how to achieve this targeted level of protection. As part of this, it's essential to understand that the journey must include file protection.

CDR is key to ensuring that all files entering or moving within an environment are safe by design, free from malicious code, structurally sound, and compliant with zero trust policies. It removes the guesswork from threat detection and delivers consistent, policy-enforced security that aligns with the military's evolving operational and cybersecurity demands.

To learn more, visit www.glasswall.com.

To schedule a demo, contact Kelly Davis at kdavis@glasswall.com.



*Breaking Defense thanks Glasswall for supporting this editorial eBRIEF.
Sponsorship does not influence the editorial content of the eBRIEF.*