SPACE

Paris Air Show »

BUSINESS

Defense Budget 2026 »

GLOBAL

MULTI-DOMAIN

PENTAGON

News Video: The Weekly Break Out »

CONGRESS

NETWORKS & DIGITAL WARFARE, SPONSORED POST

NAVAL

AIR

LAND

FEATURED:

Countdown to 2027: Where to Start Implementing the Zero Trust Strategy for the Department of Defense

By BREAKING DEFENSE on February 27, 2023 at 2:24 PM

Defense Department organizations have four years to deploy seven pillars, including 45 core capabilities of zero trust.

in \searrow

presented by **maximus**

NETWORKS

Future of the F-35 »



With the release of its Zero Trust Strategy and Roadmap in late 2022, the Defense Department (DoD) has brought clarity to a methodology that strives to ensure the perpetual security of networks, applications and data. In one use case, zero trust addresses the vexing problem of preventing attackers or malicious insiders from

moving laterally through the enterprise after they've breached endpoints and

networks. Often, these hackers operate unfettered for months before they're discovered. A well-conceived zero trust methodology minimizes the impact of the breach by isolating the resources available to the attacker. Overall, it ensures that legitimate users gain access to authorized resources based on recognized devices and appropriate circumstances. Zero trust updates the traditional idea of access through perimeter security to one of continuous security throughout the enterprise.

With its new zero trust strategy, DoD provides a blueprint to bring this cybersecurity capability to the DoD Information Network, including NIPRNet and SIPRNet, by fiscal year 2027. This will affect nearly 3.4 million DoD personnel who have unique identifiers, varying degrees of network and data access, and always-changing roles with rotating commands. For technical and program level leadership in the DoD, this presents the challenge of quickly developing roadmaps, modernizing technology, and updating processes, all while the department continues to execute its mission.

ADVERTISEMENT

The successful rollout of a program of this scale will encompass all cloud, multi-cloud,

and on-prem enterprises, which can only occur when systems have the flexibility to

accommodate change. The seven definitive pillars and 45 core capabilities identified

think differently as they deploy new technologies. Bring-your-own device (BYOD) and

the Internet of Things (IoT) connectivity are possible because well-crafted policies

establish access controls with context. Moreover, enhanced speed and scale occur

in DoD's strategy will lead to robust cybersecurity because they push agencies to

because of automated identity validation throughout the enterprise. DoD's deadline and a strong zero trust strategy are a good start. Where to begin has become the first question that many mission leaders ask. Zero Trust 2027: Start with the User Pillar

program offices begin or continue their zero trust

After reviewing the details of DoD's strategy and

implementations, Maximus recommends that DoD

understanding what's required with zero trust

journey by building out the user pillar. This element controls network and data access through privileges and policies, so it's central to the entire strategy framework. "The other six pillars of the strategy all refer back to the user pillar for validation, so identity is essential to verification of everything," said Kynan Carver, DoD Cyber Lead at Maximus. "That means verification of what data you're accessing, the resources being

As DoD agencies embrace the zero trust strategy, they will need a structured approach to meet overall objectives and especially to understand the details in the user pillar. Four years is a short time for agencies to implement a plan with multiple pillars in an environment where some agencies have more funding to dedicate to zero

trust. Maximus, with its history of modernizing large enterprise programs and

requested, and confirmation of network segments requiring access. The system must

know who signed in and what access is authorized under predefined conditions."

Kynan Carver, DoD Cyber

Lead at Maximus.

security, employs a methodology with multiple assessments to determine the maturity level of the enterprise and its vulnerabilities.

each of the core capabilities in the user pillar:

requirements to ensure policy compliance.

by a group they belong to.

been compromised.

Follow a Proven Methodology

"Implementation of a zero trust architecture begins with a clear understanding of what exists in your organization," said Carver. "It's fundamental but very labor intensive to go through Active Directory, for example, and identify every user and non-person account, then figure out why they exist, whether they are redundant, and finally determine the permissions they have versus the ones they actually need." In the DoD strategy, the user pillar lists several capabilities that every agency and program office must take into account as they develop their own roadmap. From its

1. Inventory. Know the assets that connect to the enterprise as well as user identifications and non-person identifications, such as those authorized to perform administrative functions. These will inform the gap analysis of what's needed vs what is currently operating. 2. Conditional user access. Define how users will connect to network resources. Even a role-based structure should have tiered levels so that individuals can access data and applications based on who they are, not

engagements with DoD agencies, Maximus offers the following recommendations for

4. Privileged access management. Establish just-in-time access that limits administrators' authority. Their access would be removed when they are finished with the task and resource, until they need to request new access. 5. Identity federation and user credentialing. Expect context-based

3. Multi-factor authentication. Specify any token-based processes or other

publish user and non-user identities across agencies. But before zero trust matures to that level, the other agencies will need similar policies and processes when it comes to user authentication. 6. Continuous authentication. Enhance the ability to deploy behavioral and

contextual identity verification using artificial intelligence and machine

learning. If users drastically change their patterns of activity on the

network, the technology can raise a caution to see if the account has

7. Integration of Identity, Credential and Access Management (ICAM). Plan

security policy across all of government. When this happens, DoD will

on ICAM to evolve so there is a central organization controlling processes and identities. The Common Access Card (CAC) has been a positive step in this direction, but the next generation ICAM will make it easier for agencies to manage identities, focus on users, and limit exposure to critical data. The Maximus methodology was developed to reveal the many combinations and

outcomes of activity that can lead to security gaps across an enterprise. This

approach extends to other pillars of the zero trust architecture such as data,

applications, devices, and networks. Taken together, the results of the assessments

inform agencies about their place on the zero trust journey and what to prioritize.

DoD has had the benefit of the Maximus methodology for before. For the Compartmented Enterprise Service Office (CESO) of the Defense Information Systems Agency (DISA), the company strengthened the agency's cyber defenses and increased security operations center effectiveness by 50 percent. Maximus's systems experts also supported DISA with analysis, roadmap development, an agile framework, as well as program execution during a migration to the cloud.

boundaries and offer FedRAMP-compliant solutions presents a compelling way to protect assets and mitigate evolving cyber threats."

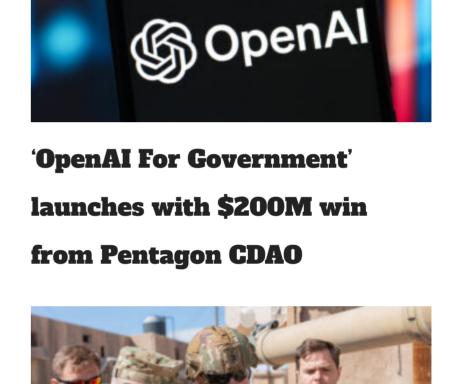
"We have a cadre of solution architects who provide secure solutions with emerging

management. "Our ability to implement a zero trust architecture within FedRAMP

technologies across DoD," said Harsha Rao, senior manager of service delivery

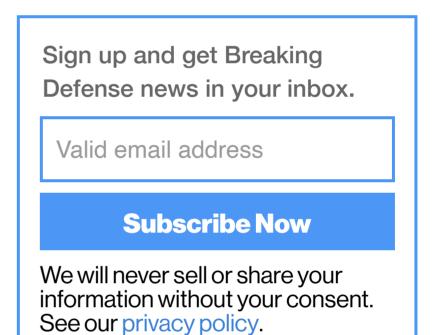
HONORING AMERICA'S HEROES HELP A VETERAN IN NEED WHEN YOU CHECKOUT AT LOWE'S





Recommended

Army seeks hefty boost in network funding in Pentagon procurement proposal



Raju Ranjan, an engineer from the AFNet Sustainment and Operations Branch, discusses plans for zero trust architecture with Capt. Christopher Kodama, a branch engineer, at Hanscom AFB. Photo courtesy of US Air Force. **Enhance the User Pillar with Customer Experience** The foundational user pillar and overall zero trust

trust checks and balances will be an adjustment for users, which DoD recognizes.

strategy offers a refreshing perspective of how DoD

of leadership, the availability of technology and

agencies will address cybersecurity. The endorsement

expertise to implement zero trust are a precursor to

impactful mission outcomes. However, the best path

capability to the user pillar: customer experience (CX).

to mission success would be to add another core

Working everyday with systems infused with zero

According to David McKeown, DoD's deputy chief

information officer, the strategy includes efforts to

build "a culture of zero trust at DOD and an

integrated approach at the department and the

component levels." Far from being mutually exclusive, zero trust and CX work together to build that culture of security in three ways. First, a well-designed experience offers simplicity within a complex program that needs clear language and navigation based on human-centered design principles. Second, intentional CX includes automation for seamless transitions across the enterprise as long as they fall within the requirements of the zero trust policies. Finally, an effective program implementing CX has the necessary checkpoints to

that the systems and data they access are secure. When users are included in the experience design, development and optimization processes, a CX approach accelerates their embrace of new processes and policies.

create trust among users who must have confidence

cybersecurity with strong user experience embedded into the systems and processes that will last for generations." X Topics: cyber, cyber security, Defense Information Systems Agency, DISA, DOD, networks,

Presented by Maximus, sponsored content, technology, Vantage Maximus, zero trust, zero trust

"The user pillar offers the greatest benefit to zero trust," concludes Carver, "because

it helps define the requirements for the other six pillars. This ultimately results in a

reduction in attack surface, a more manageable enterprise, and a new era of

Latest from Breaking Defense

model

Creating decision advantage for defense agencies through a platform approach

US support for international engagement sees jump in Reagan **Foundation poll**

Midnight Hammer: How the US conducted surprise strikes on Iran

Operation

award Ask Sage \$10M for **GenAI** expansion

Pentagon AI

office, Army

Copyright © 2025 Breaking Media, Inc. All rights reserved. Registration or use of this site constitutes acceptance of our Terms of

DEALBREAKER

Privacy Center | Do not sell my information

DMCA.com COMPLIANT

Advertising & Marketing Solutions

MedCity News

OUR

SITES

ABOVE THE LAW Service and Privacy Policy.