GovCIO MEDIA & RESEARCH

WINTER 2023

DeepDives

Implementing ZERO TRUST for the Modern Work EXPERIENCE

INSIDE:

SPONSORED BY

zscaler™ Microsoft

GovCIO MEDIA & RESEARCH

From the writer's desk

Kate Macri, Deputy Editor

Zero Trust Enables the Workforce of the Future

A zero trust approach to cybersecurity allows employees of federal agencies or private companies to work from anywhere without compromising data or network security. The COVID-19 pandemic accelerated zero trust adoption due to necessity, but for many organizations, zero trust is now an operational imperative.

Whether you're an administrative employee at a health agency or a soldier on the ground in a combat zone, zero trust allows you to connect to information services securely. This has enormous ramifications for government and industry alike: for organizations such as the Defense Department, military services can share information across teams more efficiently and effectively so they have the most up-to-date data they need to do their jobs well. For health and civilian agencies, zero trust allows for flexible work hours and locations to accommodate employee needs, all while maintaining a strong cybersecurity posture.

While zero trust is a strategy rather than a product, government and industry are working hand-in-hand to develop interoperable zero trust solutions to secure cloud-based services in remote or hybrid environments. The result? Dramatically improved mission performance.

Table of Contents

Kate Macri,
Deputy Editor

Sarah Sybert,
Staff Writer

Army Cites Data, Culture for Zero Trust Success

The Army's Unified Network Plan and Data Plan are driving zero trust implementation, but workforce training and education are key.

BY KATE MACRI

The U.S. Army plan to shift to a zero trust cybersecurity model hinges on workforce training and good data management, according to senior leadership and innovators developing zero trust solutions and laying the groundwork for the department-wide shift.

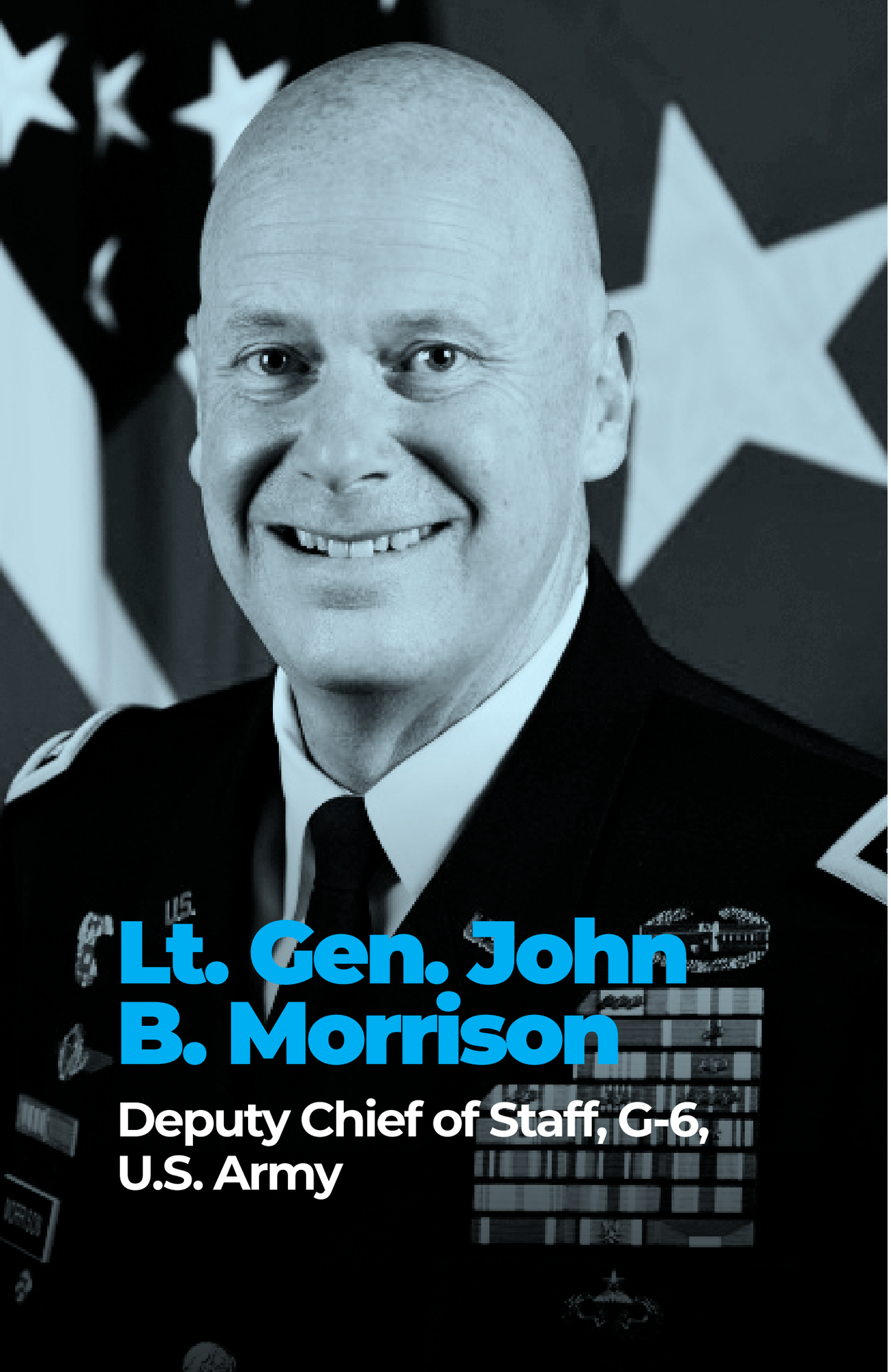
"This has got to be a comprehensive approach, it's people, it's processes, it's capabilities, and last but probably not least it's about culture," said Lt. Gen. John B. Morrison, deputy chief of staff for cyber (G-6) in an interview with GovCIO Media & Research. "Too many times people get stuck on things and that's not what zero trust is really about."

Defense cyber leaders repeatedly say culture is the key enabler for zero trust. Educating and training soldiers to think with a zero trust mindset will help them win future fights, Morrison said.

Zero trust requires a dramatic cultural shift in the way the Army and the rest of the Defense Department thinks about cybersecurity. Zero trust means shifting from a passive, network-centric model, where you establish a network perimeter and wait for the adversary to attack, to a data-centric model where administrators can restrict data access and users and devices must constantly verify their right to access data.

(ctd.)

Photo Credit: Jenna Mozeyko/U.S. Army Combat Capabilities Development Command C5ISR/DVIDS



Zero trust isn't a budget line item or a program of record, Morrison said, it's a reframing of the cybersecurity mindset.

"To make sure we're protecting the data, to do that we're ensuring who is on the network and who has access on the data, we're really thinking about the people and the training we're providing them," Morrison said.

Workforce Training for Zero Trust

The Army Cyber Center of Excellence is gearing up to release a zero trust curriculum to train soldiers on the zero trust cybersecurity model later this year.

The center's Command Chief Warrant Officer Paul Sankey said Chief Warrant Officer 3 (CW3) Benjamin Koontz was the first to implement zero trust in a tactical environment in 2020.

Koontz worked at the Defense Information Systems Agency (DISA) for three years and, while there, worked on zero trust prototypes with the National Security Agency (NSA) and at CYBERCOM's innovation hub, DreamPort.

"We utilized the currently fielded equipment, so whatever gets fielded on our tactical server infrastructure TSI stacks, and we looked at that and figure, how do we take what we currently have and put zero trust around it?" Koontz told GovCIO Media & Research in an interview.

To test the zero trust controls, Koontz set up on various Army devices, he organized four separate red team events to try to penetrate the devices and extract data.

"We were extremely successful on all four events," he said. "One time they utilized trusted insiders with administrative permissions. Another time they took one of our devices and uninstalled all of our security tools with an instructed insider, and another time they utilized a close action team to try to get into facilities, and they utilized the trusted insider to help them get into other facilities and all those times they failed. We were extremely successful on stopping that. So now going forward with that implementation that we did, we

took the lessons, and we're building guidance to other organizations to say hey, these are things that all the other technical organizations within the Army can do as well."

Due to the success of Koontz's prototype, the Army Cyber COE Commanding General Maj. Gen. Paul Stanton recruited Koontz to develop training for soldiers.

"A lot of organizations [within the Army] are leveraging his expertise and experience in that realm," Sankey told GovCIO Media & Research. "A lot of the pilots revolve around him assisting the divisions and other organizations. He's working with the 101st Airborne Division to implement control concepts on their tactical network using that guide and scorecard with the specific goal of improving those so that once it's fully developed, it can be provided to [the Department of the Army] for distribution across the entire Army."

Morrison said the COE is helping the Army "change our processes," which is critical for the shift to zero trust to be successful.

"Zero trust isn't something you buy, it's a journey," Army Acting CIO and CDO David Markowitz, said in an interview.

Data Anchors Zero Trust

Culture and workforce training constitute one piece of the zero trust puzzle, but Army cyber leaders believe good data management and governance are also critical for any zero trust approach to be successful.

Markowitz said the Army Unified Network Plan and Army Data Plan are the two engines driving zero trust implementation at the Army in accordance with the DOD's recently released five-year zero trust strategy.

"General Morrison was talking about the people, but there's also a data component," Markowitz said. "So the Army has a data plan to make sure if we get the right view of who is in the Army and who has the right to see what data and has the right credentialing … [and ensure] we've got the right tagging of the data so that those can marry up, so we can control access at a granular level." (ctd.)

Photo Credit: amgun/Shutterstock

The Army is now in the third year of implementing its data strategy. The first year, Markowitz said, focused on establishing a data enterprise governance plan.

"The main goal is to simplify the data landscape," he said. "Just tag what's important and focus on cybersecurity for what's important, for management control. That data lifecycle management is a key component of our governance."

Army Secretary Christine Wormuth highlighted data-centricity as one of her primary objectives for the Army last year.

For Morrison and Markowitz, zero trust and data-centricity are symbiotic. Data readiness is necessary for zero trust to be successful and vice versa.

"There is no data centricity without applying zero trust," Morrison said.

Zero Trust Role in JADC2

Joint exercises with the sister services for the Defense Department's Joint All-Domain Command-and-Control (JADC2) initiative and the Defense Information Systems Agency's Thunderdome zero trust prototype are also helping the Army hone its zero trust implementation and training plans.

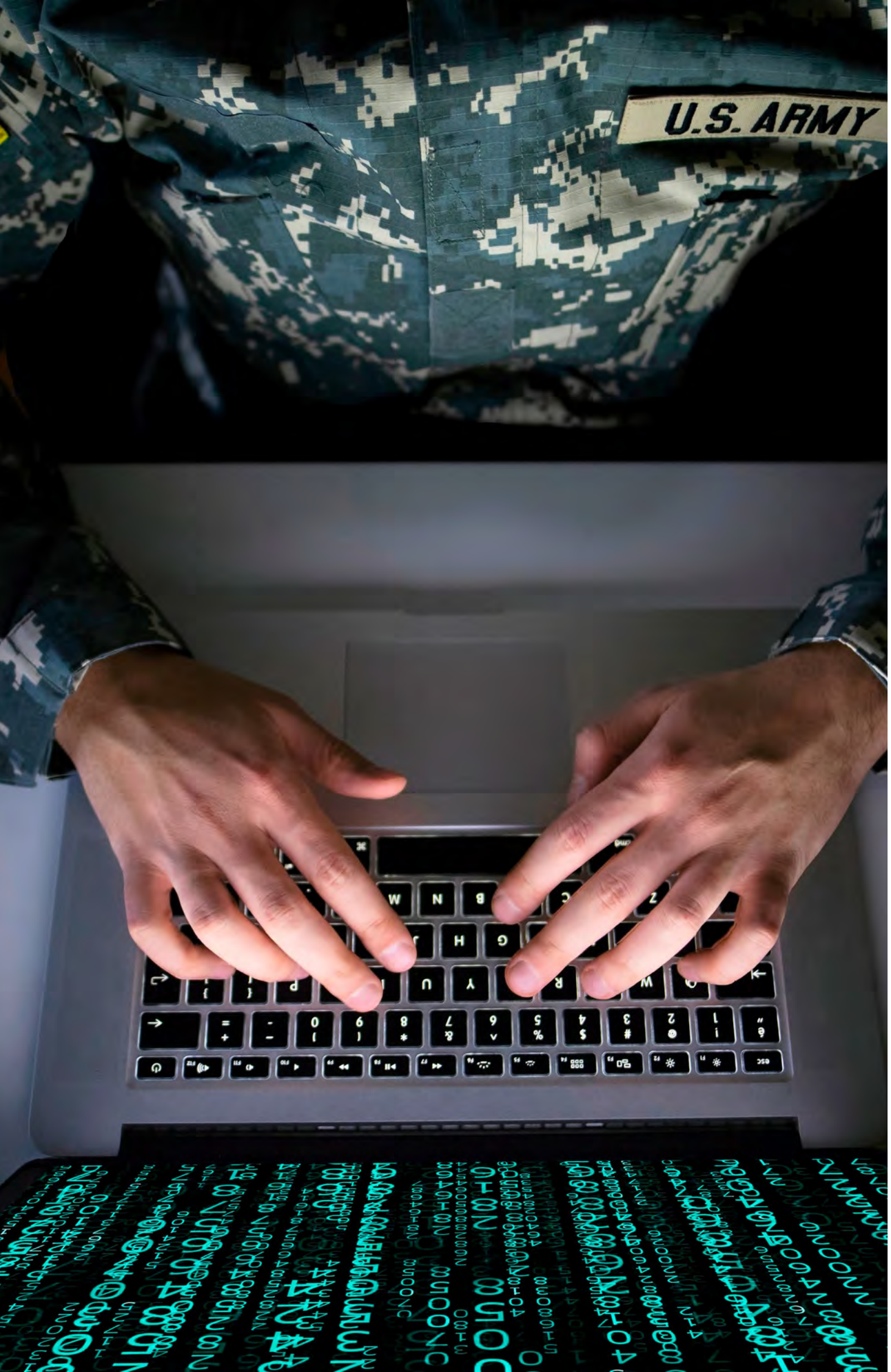
Morrison and Markowitz said they saw zero trust use cases and lessons learned come out of Project Convergence, the Army's contribution to JADC2.

"Project Convergence has many benefits to the Army, this is just one component of it," Markowitz said. "Understanding what data is needed for a specific mission, trying to tag it appropriately … zero trust should be inherent so they can rapidly decide [securely]. It's a critical component for our operations and for understanding our network under an adversarial attack. This network reform is critical."

The Army is currently working through how to iterate those lessons learned while maintaining interoperability with the other military service branches.

"We're putting that same kind of iterative process in place specifically focused on data operations into an operational theater, mainly with U.S. Army

Photo Credit:
Gorodenkoff/Shutterstock



Pacific," Morrison said. "Key to that is also how are we doing that iterative development and learning of applying zero trust principles so we can move toward this notion of being a data-centric Army and how that will actually support us conducting military operations, but also being very user centric in our design, putting it with an operational formation where we can bring all of that together, really focused on data, but applying zero trust principles so we can iterate and learn and figure out what that looks like and then apply it more broadly across the Army."

DISA's Thunderdome zero trust prototype also highlighted the importance of data interoperability between the services for the kind of secure, rapid data exchange JADC2 requires.

"From the data side, the DISA folks, because they had to wrangle with the processes that are different across the services, it was very insightful to hear from DISA how they had to wrangle the processes to get to a common view of the data for identity management, core to zero trust principles," Markowitz said.

Morrison said the Army will meet with DISA in a series of sessions in the coming weeks to discuss next steps for zero trust implementation.

"[Zero trust is] absolutely central to everything that is JADC2," he added. "At its core, [JADC2 is] how fast can we pass data [securely] amongst the joint forces and our coalition partners."

Photo Credit: Aleksandar Malivuk/Shutterstock

“This has got to be a comprehensive approach. It’s people, it’s processes, it’s capabilities, and last but probably not least it’s about culture. To make sure we’re protecting the data, to do that we’re ensuring who is on the network and who has access on the data, we’re really thinking about the people and the training we’re providing them.”

— Lt. Gen. John B. Morrison, Deputy Chief of Staff, G-6, U.S. Army

GovCIO MEDIA & RESEARCH

DeepDives

Zero Trust for a Hybrid Workforce

Zero trust can improve user experience in a hybrid work environment without compromising cybersecurity or mission integrity.

8 Pillars of Zero Trust

- Users
- Devices
- Network
- Infrastructure
- Applications
- Data
- Visibility
- Automation

PARTNER INTERVIEW

zscaler™ Microsoft

Securing Cloud Services with Zero Trust for Modern Government

Zero trust principles work in tandem with FedRAMP to enhance cloud security and improve user experience for federal agencies adapting to hybrid workforce models

Luis Mendoza
Sr. Director of Business Development, Microsoft Alliance Lead, Zscaler

Jose Padin
Public Sector Chief Transformation Officer, Zscaler

What are some challenges around securing a hybrid work environment or telework environment, and how can zero trust play a role in mitigating these challenges for modern work and a seamless user experience?

Mendoza In a hybrid work environment, zero trust requires that agencies would enable their employees, contractors, vendors and customers to securely collaborate on their resources. This means allowing them to access from wherever they want, whenever they want, using whichever device, network, application they want, either internally or externally managed apps, all while meeting industry standards and government regulations. All of this can be a daunting task. This is precisely why, through a cloud-native approach through zero trust, which is combined in the backhand with advanced technologies like artificial intelligence (AI) and machine learning (ML), can help agencies overcome expectations and security risk. The

future success of agencies hinges on providing productive and secure access to the agency's digital resources, so it's really paramount for them to make themselves more competitive through a zero trust framework.

Padin To add on to what Luis talked about, being able to connect a user to any device and be able to do that securely is really critical as we move forward in this hybrid work environment and should be able to give you consistent infrastructure as well. If you're having to create a hybrid work environment for system A, a different one for system B and a different one for system C — that kind of a siloed approach to the hybrid work environment can create a lot of confusion for the users and a lot of challenges across an agency.

Looking for a platform that can take in multiple different scenarios, different experiences and different applications and be able to give a consistent user experience is really critical to help reduce the challenges of this hybrid work environment going forward

Zero trust has only recently become a major cyber-security trend within federal agencies. What are common misconceptions around zero trust, and how are you breaking through the noise?

Padin The first misconception I've found is that the government is working toward or building toward or looking at zero trust. Those were correct terms four years ago, but coming through the pandemic it was incredible to see how fast the government moved to change operations. Today we have multiple large government agencies who have zero trust principles in play. It's in production; it's not something that's going to happen or is happening, it's something that has happened.

The second misconception is that zero trust requires a massive change, re-architecture and redesign, and that we need to spend multiple years to get to zero trust. Because of the simplicity of some of the solutions and the way

"We're not moving to zero trust because it's a trend or cool to do. We're moving to zero trust because the on-premises castles we've built for many years — and I've built many over the last 20 years — have shown they are insecure and an attack vector of their own. We have to do something different."

— Jose Padin, Public Sector Chief Transformation Officer, Zscaler

you can quickly add in zero trust principles into existing architecture, you can get wins in the near term or short term. It doesn't require a five-year program of ripping and replacing.

We're not moving to zero trust because it's a trend or cool to do, we're moving to zero trust because the on-premises castles we've built for many years — and I've built many over the last 20 years — have shown they are insecure and an attack vector of their own. We have to do something different. We can't keep building taller and taller castle walls when they're being compromised again and again. Zero trust is a natural evolution of cybersecurity and architecture design, its current rollout in federal and those principles will reduce attacks. Zero trust is a team sport. It takes many vendors to have a zero trust solution that's effective, and Microsoft is a great partner to have in that effort.

Mendoza Something we continue to see is that zero trust is already a reality from Zscaler's perspective. This technology is already being widely adopted. It also means that customers can now really start to use this as a tool to help themselves differentiate in the marketplace and make their own employees more productive. When you think of software-as-a-service (Saas) applications and other applications within the cloud ecosystem, we see them fitting together more quickly, more often. So you have to continuously keep building that zero trust native approach to the larger framework so that when you go into a secondary or third party set of applications, you have a flexible framework that helps you build and expand and keep delivering the level of security that you need while ensuring that productivity is in place.

How do cybersecurity solutions around zero trust dovetail with FedRAMP requirements for federal agencies? What does zero trust look like in cloud service offerings at low, moderate and high FedRAMP impact levels?

Padin FedRAMP is a critical component of being able to modernize our security. The reason why is because if we created a new government agency tomorrow, we wouldn't go down the route of building a lot of infrastructure in a physical location. We would've done that 10 to 15 years ago no doubt, but in 2023, we're going to build a modern architecture that is built on cloud services.

So how do we determine how we use these cloud services? We need some type of third party to determine whether the services we're putting together meet security requirements from the client's perspective. And that's really

Photo Credit: PopTika/Shutterstock

what FedRAMP provides everyone — that is, an ability to say it's not just the vendor, it's a third party that has done an assessment of the SaaS, allowing us to move more quickly in implementing and getting the benefits of SaaS in federal government.

When it comes to the impact levels — when we talk about high, what obviously really drives this is the FISMA data designation for handling higher level data. Traditionally, that would drive us to build enclaves by bringing those servers on-premises. But now, if I am using the principles of zero trust, and I want to reduce the management of hardware on-premises, I want to look at cybersecurity solutions that are built as SaaS and take my security out of the castle-and-moat approach and bring it to the cloud. That's the trend that we're seeing. Zscaler's FedRAMP high impact level accreditation allows me to use solutions that reap the benefits of using modern cybersecurity principles, including zero trust.

What are some examples of how zero trust can enhance cybersecurity through strict yet flexible access controls and simultaneously improve user experience and ease of access in a cloud environment?

Mendoza The key word is user experience. In that context, cloud-native zero trust is a gamechanger. They want to do it in a single click from their device. When it comes to our advanced Microsoft integrations, for a user whose job depends on analyzing real-time data that is hosted on the internet, they can do so while mitigating the underlying security risks.

We handle over 270 billion transactions a day. Most of this is real-time traffic, which is largely complementary to what Microsoft sees directly. So this means we are exposed to a significant amount of attack vectors. When we identify anything that seems to be a potential zero trust threat, we take that suspicious file and we detonate it in a cloud sandbox environment. If we confirm this is indeed a real threat, we will then in the back end communicate to the defender through an API, and this allows Microsoft Defender for Endpoint on the other end to alert the IT department so they can take remediation actions and isolate the systems that have been exposed to this and prevent the threat from spreading to the larger fleet. This also creates an indicator of compromise, which then is going to benefit not only the particular agency in near real time, but also all of Microsoft's customers at large.

Image Credit: pinkeyes/Shutterstock

zscaler™

Microsoft

Modernize your agency securely. Trust the **One True Zero.**

Safeguard your hybrid workplace and accelerate digital transformation.

FedRAMP

Learn more at zscaler.com/federal

Zero Trust is Key to Hybrid Federal Workforce

Agencies are bolstering workforce training and zero trust to secure the hybrid workplace.

BY SARAH SYBERT

Federal agencies are embracing the hybrid workforce to attract talent and boost employee morale, but cybersecurity — and zero trust — are key to the longevity and success of this model.

Between 2019 and 2021, the number of people primarily working from home tripled from 5.7% to 17.9%, according to the U.S. Census Bureau. The Office of Personnel Management's (OPM) 2022 Federal Employee Viewpoint survey found only about one in three government workers work from an office five days per week.

Some agencies are taking advantage of these new realities. The Department of Veterans Affairs, for example, is offering perks such as remote work and special pay rates to attract tech talent and compete with industry.

"Over 62% of our IT workforce is working remotely. We are going to continue to expand as we modernize our workforce," VA Deputy CIO and Chief People Officer Nathan Tierney told GovCIO Media & Research. "Data, AI and other advanced techniques that you see in the private sector, we need to bring into the public sector if we're going to achieve the vision of being a world class IT organization."

As government looks to increase remote positions to attract top talent, agencies are reevaluating what it means to be "secure" in the new workplace. That's where zero trust comes into play. (ctd.)

Photo Credit: Thapana_Studio/Shutterstock

The Move to Zero Trust

Zero trust is not a product or a service, but a strategy. Instead of relying on a perimeter-based approach, every user, device and app must be verified for every point of access.

President Joe Biden's May 2021 cybersecurity executive order ignited the transition to zero trust architectures, which led to the expansion of tools such as identity, credential and access management (ICAM) solutions, data governance and automation.

"The recent legislation has really brought into focus some very key initiatives for all federal agencies," VA CISO Lynette Sherrill told GovCIO Media & Research in a recent interview, which will be featured on CyberCast in March 2023. "All throughout fiscal year 2022, we made some significant advancements with deployment of endpoint detection and response capabilities. We also implemented and improved our security vulnerability management program. We're now able to say that we have more than 93% of our vulnerabilities managed on our network, well above industry standard of about 70%."

Following the zero trust executive order, federal agencies began developing and implementing zero trust strategies, including the Defense Department's five-year zero trust strategy and VA's Zero Trust First Cybersecurity Strategy, to provide guidance and measures to effectively secure agency assets.

VA is developing a roadmap to get to zero trust, which enables the agency to take a holistic approach to its cyber posture. VA also requested a $107 million increase to its fiscal year 2023 cybersecurity budget to provide more funding to its information security program, focusing on implementing zero trust principles.

VA CIO Kurt DelBene said he is focusing on a zero trust framework to develop a set of measures of security and inform decision-making moving forward.

"There's nothing more important than securing the organization, securing the assets that we have, and — at its heart — it's about securing veteran data, which is our commitment to them," DelBene said during a Sept. 30 media roundtable.

Training and Recruitment

Change management is critical to developing a "security first" mindset across the federal workforce.

The Defense Department's newly released 2023-2027 DOD Cyber Workforce Strategy is built around four tenets: performing capability assessments and

Photo Credit: oumjeab/Shutterstock

analysis processes to stay ahead of force needs, establishing an enterprise-wide talent management program, facilitating a cultural shift within the department, and developing partnerships "to enhance capability development, operational effectiveness and career broadening experiences."

"We need a dedicated workforce strategy … looking not only at cyber, but broader STEM efforts, and what we're doing across the enterprise era. So, we have a strategy specifically on this as we look to diversify the workforce … this really is our generation space race," DOD CIO John Sherman said during the September 2022 Billington Cybersecurity Summit.

Workforce training and recruitment is also top of mind as the Department of Commerce continues to accelerate security. By focusing on the people, agencies will be able to better account for identities and devices accessing networks.

"It comes down to the people first when it comes to cybersecurity and ensuring that risk model — people, people, people — that's what's so most important," Commerce's Bureau of Industry and Security CIO Nagesh Rao said during GovCIO Media & Research's July 2022 Blueprints of Tomorrow virtual event. "I'm noticing it with my CISO team and my colleagues in the cybersecurity area that it's education, awareness and understanding."

VA's zero trust journey relies upon integrating zero trust principles within the workforce, DelBene said during GovCIO Media & Research's September 2022 Zero Trust event.

"We reworked the team and set a vision of being vision oriented, having great execution operational rigor, security rigor and focusing around a delightful end-user experience," DelBene said.

DelBene acknowledged zero trust as a powerful framework for security. If it's implemented well within an organization, the workforce should understand the key principles inside and out. Security should be a part of an employee's passion and how they approach their work at the agency, he added.

"First thing we should do is get a workforce that fundamentally believes

security is the most important thing," DelBene said. "The people driving your system need to have a sense of what zero trust means to them. Designers and developers have to have that inherent thought that security is at the core of what they do."

Sherrill said VA uses tabletop exercises and simulations to prepare the workforce to respond to breaches and drive an Agile approach to security. The agency also holds an annual cybersecurity and privacy training that all employees and people accessing VA's network are required to complete.

"My mantra with the team lately has been if we have a [security] event, or even if we hear of an event that's happening in industry, that we take that, we bring it into our environment, and we try to learn from it so that we are more secure on the other side of that event than we were going into it. So, let's constantly be learning and improving everything that we do today."

Identity Management: A Critical First Step

Identity management techniques such as multifactor authentication (MFA) and least privileged access are core tenets of zero trust. The Department of Health and Human Services (HHS) and VA are focusing on identity management to

Image Credit: PeachShutterStock

build resilient IT infrastructures, sustainable even in a remote or hybrid environment.

Sherrill said VA has enforced MFA with 96% of the agency's end user community.

"Zero trust is really at the heart of our cybersecurity strategy. And what that means is we enforce strong identity verification. So, [for] every end user on our network, we know who they are and where they're authorized to go," Sherrill said. "We also ensure that the devices connecting to our network are healthy, meaning they haven't been compromised, they have all the latest patches, they have all the latest security configuration."

Former HHS Office of the Inspector General CIO Gerald Caron, who recently took on a new role as CIO of the International Trade Administration, said authentication is critical in the hybrid work environment. Different methods of identity proofing lead to varying levels of risk.

"When I come up with my confidence score, how much I trust that common access card (CAC) or personal identity verification (PIV) card is going to probably have a lower risk than your username, password or some other methods of authentication," Caron said during an event last year. "That will depend on what I'm going to allow you to do … once you get to that authoritative identity, you can start to look at automation of the provisioning and deprovisioning."

Remote work also increases the number of devices on agency networks. Bring-your-own-device (BYOD) programs enable employees to connect their personal devices to employer networks and access work-related systems and agency data.

The Department of the Army, for example, is preparing to roll out its BYOD program to about 20,000 soldiers and civilian employees. During a CyberCast interview with GovCIO Media & Research, Lt. Gen. John Morrison, the Army's deputy chief of staff, G-6, said the BYOD program aligns with the larger Defense Department effort to allow service members and civilians to work on their

phones and home computers. Now, the focus is on user experience and security.

"We really have sort of inside our Army flipped the paradigm of how we look at the problems. Instead of cybersecurity being something we bolt on at the end, that's really not a good way to approach it. We bake it in on the front end," Morrison said. "With bring your own device, that's exactly what we've done. And the technical instantiation is, while there's an application that resides on your phone, none of the data does. It's still all resident in the cloud with the appropriate defensive cyber watch over the top of it."

"Zero trust is really at the heart of our cybersecurity strategy. And what that means is we enforce strong identity verification. So, [for] every end user on our network, we know who they are and where they're authorized to go. We also ensure that the devices connecting to our network are healthy, meaning they haven't been compromised, they have all the latest patches, they have all the latest security configuration."

— Lynette Sherrill, CISO, Department of Veterans Affairs