Fall 2021

ON THE FrontLines MAGAZINE

ZERO TRUST ARCHITECTURE *in Government*

Q & A

SCOTT ROSE

NIST Zero Trust Lead
Co-Author of NIST 800-207
page 8

Plus

"How To" ZTA Info from…

- NSA
- CDC
- Army Corps of Engineers
- Education
- ACT-IAC
- DLT
- Lookout
- CyberArk
- Fortinet
- Illumio
- Okta

Zero Trust Architecture (ZTA) — Not A Widget; It's A Framework…

Ultimately being able to access critical information securely – whether you are sharing it with other mission partners or using it internally – is the ZTA goal.

Recent cyber and ransomware attacks have made it imperative that federal, state and local governments and the private sector work together to simultaneously implement ZTA environments ASAP.

The May 2021 Executive Order makes clear that modernizing our current digital situation is a moral imperative and that failure is not an option.

So, with all of this talk about Zero Trust and Zero Trust Architectures, what exactly are we talking about?

According to the IT executives featured in the pages that follow, ZTA has some guiding principles including:

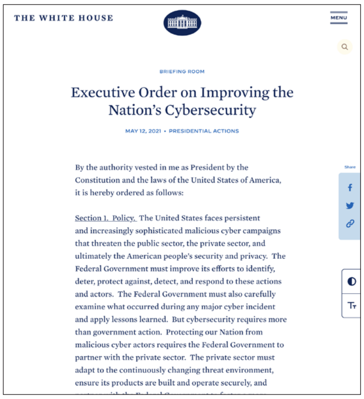
- ZTA is a philosophy and set of security principles based on the acknowledgment that we need to re-think security from the ground up.
- Agencies need to implement ZTA controls across these six foundational elements: identities, devices, applications, data, infrastructure, and networks.
- ZTA refers to an evolving set of security paradigms that narrows defenses from wide network perimeters to individual or small groups of resources.
- ZTA is not a product or specific technology and the advent of cloud computing offers a rare chance to deploy completely new IT models as well as security.
- ZTA verifies and authenticates user and device identify before every application session to confirm that they meet the organization's policy to access that application, and grants the least privilege necessary to perform the task at hand.
- ZTA relies on having robust monitoring in place to react quickly to changing network conditions or newly discovered threats.
- The main attribute of a successful ZTA program is getting full buy in from senior leaders all the way down to those engineers, architects, administrators who implement ZTA capabilities.
- ZTA is more policy-based and requires a lot more upfront thought not just from the security types, but from leadership as well on what access, what data, what devices are approved for that user.
- ZTA is simultaneously a concept, a framework, an approach, an architecture, a set of guiding principles, a systems design, and an operational model to cybersecurity and risk management.
- To do ZTA right is to touch every element of the 7 layer model. That's not just networks, that's an architecture.

ZTA is a paradigm change so use NIST SP 800-207 as your guiding North Star to implement your own ZTA Architecture (ZTA) capability within your own environment. ■

Executive Order on Improving the Nation's Cybersecurity
May 12, 2021

Sec. 3. Modernizing Federal Government Cybersecurity.
(a) To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.

Read the complete Executive Order.



Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and

Inside Zero Trust Architecture

Embracing a Zero Trust Security Model

National Security Agency (NSA)

Executive Summary

As cybersecurity professionals defend increasingly dispersed and complex enterprise networks from sophisticated cyber threats, embracing a Zero Trust security model and the mindset necessary to deploy and operate a system engineered according to Zero Trust principles can better position them to secure sensitive data, systems, and services.

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses.

The Zero Trust security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity.

Zero Trust embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting critical assets (data) in real-time within a dynamic threat environment.

This data-centric security model allows the concept of least-privileged access to be applied for every access decision, allowing or denying access to resources based on the combination of several contextual factors.

Systems that are designed using Zero Trust principals should be better positioned to address existing threats, but transitioning to such a system requires careful planning to avoid weakening the security posture along the way.

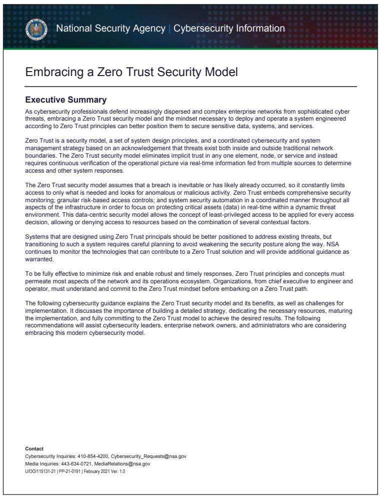
NSA continues to monitor the technologies that can contribute to a Zero Trust solution and will provide additional guidance as warranted.

To be fully effective to minimize risk and enable robust and timely responses, Zero Trust principles and concepts must permeate most aspects of the network and its operations ecosystem. Organizations, from chief executive to engineer and operator, must understand and commit to the Zero Trust mindset before embarking on a Zero Trust path.

The following cybersecurity guidance explains the Zero Trust security model and its benefits, as well as challenges for implementation. It discusses the importance of building a detailed strategy, dedicating the necessary resources, maturing the implementation, and fully committing to the Zero Trust model to achieve the desired results. The following recommendations will assist cybersecurity leaders, enterprise network owners, and administrators who are considering embracing this modern cybersecurity model.

Source: NSA February 25, 2021

[Download NSA Issues Guidance on Zero Trust Security Model.]



National Security Agency | Cybersecurity Information

Embracing a Zero Trust Security Model

Executive Summary

As cybersecurity professionals defend increasingly dispersed and complex enterprise networks from sophisticated cyber threats, embracing a Zero Trust security model and the mindset necessary to deploy and operate a system engineered according to Zero Trust principles can better position them to secure sensitive data, systems, and services.

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses.

The Zero Trust security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting critical assets (data) in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, allowing or denying access to resources based on the combination of several contextual factors.

Systems that are designed using Zero Trust principals should be better positioned to address existing threats, but transitioning to such a system requires careful planning to avoid weakening the security posture along the way. NSA continues to monitor the technologies that can contribute to a Zero Trust solution and will provide additional guidance as warranted.

To be fully effective to minimize risk and enable robust and timely responses, Zero Trust principles and concepts must permeate most aspects of the network and its operations ecosystem. Organizations, from chief executive to engineer and operator, must understand and commit to the Zero Trust mindset before embarking on a Zero Trust path.

The following cybersecurity guidance explains the Zero Trust security model and its benefits, as well as challenges for implementation. It discusses the importance of building a detailed strategy, dedicating the necessary resources, maturing the implementation, and fully committing to the Zero Trust model to achieve the desired results. The following recommendations will assist cybersecurity leaders, enterprise network owners, and administrators who are considering embracing this modern cybersecurity model.

Contact
Cybersecurity Inquiries: 410-854-4200, Cybersecurity_Requests@nsa.gov
Media Inquiries: 443-634-0721, MediaRelations@nsa.gov
U/OO/115131-21 | PP-21-0191 | February 2021 Ver. 1.0

Lookout

Protect Your Mobile Workers with Endpoint-to-Cloud Security

Your mission is increasingly tied to endpoint security as your employees telework. Tablets, smartphones, and Chromebooks are often the devices of choice when supporting diplomats, ensuring battlefield safety or enhancing citizen services in the field. Cybercriminals know this and are targeting these devices to compromise your infrastructure.

User education, awareness and a comprehensive security strategy that supports a Zero Trust approach should be standard practice for all agencies, whether their workers are in the office or teleworking.

It's time to adopt an endpoint-to-cloud approach to cybersecurity. Learn how you can protect your organization from this shift in the threat landscape by balancing privacy and security to remain nimble and compliant.

Lookout delivers Zero Trust for U.S. Public Sector agencies

SCAN HERE

Find out more at www.lookout.com/gov

NIST Q&A on Zero Trust

Scott Rose, NIST's Zero Trust subject matter expert, answers some common questions about Zero Trust.

Scott Rose
Computer Scientist, Information Technology Lab
National Institutes of Standard and Technology (NIST)

Zero Trust refers to an evolving set of security paradigms that narrows defenses from wide network perimeters to individual or small groups of resources. Its focus on protecting resources rather than network segments is a response to enterprise tends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary.

ZTA strategies are already present in current federal cybersecurity policies and programs, though the document includes a gap analysis of areas where more research and standardization are needed to aid agencies in developing and implementing ZTA strategies. Additionally, this document establishes an abstract definition of Zero Trust and ZTA as well as general deployment models, use cases where ZTA could improve an enterprise's overall IT security posture, and a high-level roadmap to implementing a ZTA approach for an enterprise. (Source: NIST)

Q. *Zero Trust is a journey and can be a complex process for many organizations, especially the smaller ones. If an organization is beginning this journey, what's your advice about how best to get started and what are some of the first steps to take that make the best impact up front?*

A. **Scott Rose:** The first, and possibly biggest step an organization takes when migrating to a Zero Trust architecture is cultural in nature. Organizations need to understand their core business processes and the risks associated with those processes. This is where an organization's security planners, workflow owners, and resource owners need to work together to conduct a comprehensive risk analysis. This comprehensive risk analysis relies on cybersecurity teams and operation teams working together to discover, audit, and monitor all aspects of the organization: identities, data, assets and data flows. A successful migration to Zero Trust requires cooperation and communication from all components in the organization. Unfortunately, just relying on documentation is often not enough as there is often a separate "oral history" and tacit knowledge of infrastructure operations that is not written down. Any cultural stovepipes between security teams and administrators and operators need to be broken down because Zero Trust relies on communication between these teams to succeed.

This knowledge of the organization needs to include monitoring current activity as well. Any audit of an organization's resources will become out of date quickly unless it includes a continuous monitoring program. Zero Trust relies on having robust monitoring in place to react quickly to changing network

Zero Trust relies on having robust monitoring in place to react quickly to changing network conditions or newly discovered threats.

conditions or newly discovered threats. Many attacks could be quickly identified and mitigated it they are discovered in the early phase of infiltration and before the exploitation phase.

Zero Trust cannot be "bolted on" to an existing IT infrastructure, but also requires a change in how cybersecurity is discussed in the organization. Simply adding common Zero Trust elements such multifactor authentication or microsegmentation will not result in a Zero Trust enterprise if the policies used to deploy and operate these elements are not updated.

Q. *NIST is famous for its Cyber Security Framework and the collaborative way that NIST reached out to partners across government, industry, academia and non-profits in order to develop a solid framework that is nationally and internationally recognized and accepted as the gold standard. How can the same set of organizations get involved in order to make this Zero Trust effort just as collaborative and inclusive?*

A. **Scott Rose:** The tenets described in NIST SP 800-207 are a conceptual framework and are slightly different than the Cyber Security Framework (CSF). The tenets are meant to be a set of guiding principles used with tools such as the CSF or the NIST Risk Management Framework to develop and implement an IT security architecture. The concepts in NIST SP 800-207 will shape future deeper dives into specific facets of Zero Trust like identity governance, internet of things (IoT) deployments in a Zero Trust enterprise, etc.

These future works will follow the usual process of NIST consulting with, and soliciting comments from, the public and private sectors and other stakeholders. Some of this work may add to or refine the existing tenets to support a specific use case or industry need. These improvements may feed a revision of SP 800-207. The Special Publication is seen as the initial work. We anticipate further refinement and improvement as the community learns more about the challenges and opportunities surrounding implementing Zero Trust architectures.

Q. *How is the National Cybersecurity Center of Excellence going to be involved in the Zero Trust effort and how can organizations gain awareness and insight into what's happening there? How can organizations get involved?*

A. **Scott Rose:** The National Cybersecurity Center of Excellence (NCCoE) is currently starting a project in policy-based resource access in a Zero Trust architecture. The project will demonstrate example implementations of a Zero Trust architecture using vendor technology designed using the approaches and models described in NIST SP 800-207. The abstract architecture in NIST SP 800-207 was used to describe the functional component requirements that can be satisfied using commercially available and open source products. The project Zero Trust Architecture builds will be used to perform a set of scenarios of resource access (e.g., employee access to resources, remote employee access to resources) The lessons learned from the builds and example implementations will be documented and used to identify areas for further work and refinement of Zero Trust definitions and concepts.

Vendor collaborators for the current NCCoE Zero Trust project have been selected and announced on the NCCoE's ZTA page (see https://www.nccoe.nist.gov/zerotrust for more information). However, there are other ways for individuals and organizations to get involved and stay informed such as joining the NCCoE Zero Trust Architecture community of interest. The community of interest is how the project will communicate updates about the project as well as announcements about NCCoE events or work related

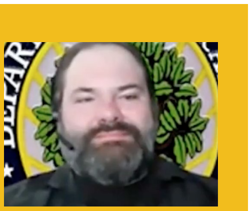
Continued on page 46

The Zero Trust Future

Zero Trust is a fundamental paradigm shift in how we think about security.

Ask Education CISO, **Steve Hernandez** about what the "Zero Trust lifestyle" future looks like and he foresees a government pushing hard towards shared services and software as a service (SaaS).

"I think we are moving to have greater separation of the trust layers; up into the point where we're saying we're actually only going to deploy trust and we're actually only going to think about trust at Layer 7," he said.



Steve Hernandez

Kevin Bingham

Dovarius Peoples

Paul Morris

This is a fundamental shift in how we think about security because we're going to have to lean really hard on our application development teams and help them get up to speed on what Zero Trust means when they are developing software as a service, Mr. Hernandez added. He predicts in the next five to ten years smart players in the field are going to handle all of this at Layer 7.

At NSA, CISO **Kevin Bingham** says that for Zero Trust the goal is simple; to make sure a single compromise will not threaten the ability to accomplish the mission.

He also sees progress within DOD where there is a better alignment between different projects and programs – and more funding. And things such as data tagging, data protection are starting to get the attention that they need.

"It's allowing us to pull from those legacy programs, manage our portfolios and manage the money better," Mr. Bingham said.

For CISO **Dovarius Peoples** at the Army Corps of Engineers, "things continue to change so we're living in what we call 'the new now'. It's not the 'new norm', it's the 'new now' because tomorrow things may completely change. To meet the end user where they are, we have to really embrace this concept of remote work."

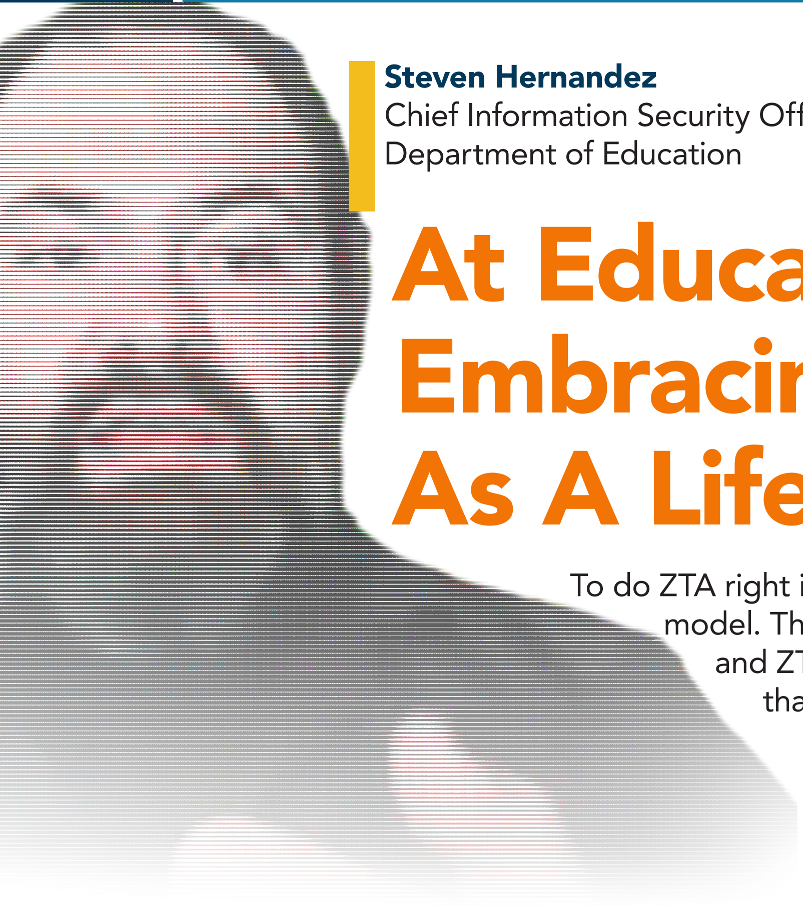
Mr. Peoples predicts that how we pursue funding from a federal perspective will probably change because being able to leverage these new technologies and capabilities is going to force us to think about things from multiple years versus just the year of execution. For him it is how to take advantage of multi-year dollars to help move modernization efforts and initiatives forward.

CDC CISO **Paul Morris** says Zero Trust is really lifestyle choice; this is a change in how we manage and provide critical services to the enterprise and our customers; it's not just that you have accounts over here, you have tickets over here, I mean it's bringing together the organization of service that is needed of IT; I see that this is going to be that standard going forward.

"What I really like is the fact that we are going to do a lot of work here based on the Executive Order to really codify architecture and direction in cloud security, software development security, supply chain security and Zero Trust; all of these things are coming together."

The playbook is coming together and "I think in two to three years a lot of that work is going to be done and documented", Mr. Morris said. "We're all going to say: well where do you fit; what are the gaps and then I can talk about what's missing instead of trying to evolve."

All this is part of our Zero Trust future. But first we have to get there. Turn the page and find out how these four IT executives are turning Zero Trust from concept to action. ■



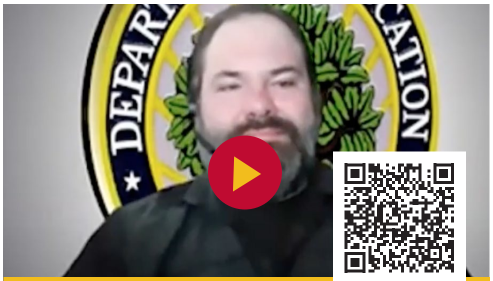
Steven Hernandez
Chief Information Security Officer (CISO)
Department of Education

At Education, Embracing Zero Trust As A Lifestyle

To do ZTA right is to touch every element of the 7 layer model. That's not just networks, that's an architecture and ZTA had to evolve to be more encompassing than Zero Trust networks.

Progress On ZTA's Four Pillars

Almost three years ago the CIO Council decided to explore Zero Trust networks. The first request was to focus on Layer 3 and see what was "the art of the possible." We pulled together government focused working groups with our friends at the NIST Cybersecurity Center of Excellence and ACT-IAC. We soon realized this is much bigger than Layer 3 and to do this right we really have to talk about the whole 7 layer model and touch every single element of it.



Mr. Hernandez comments are from the Federal Executive Forum on Zero Trust Architecture broadcast on Federal News Network.

That's not just networks, that's an architecture; and that's how we landed on Zero Trust Architecture (ZTA) versus something like Zero Trust Network. We had to evolve it to be more encompassing. At the department we have four big pillars:

First, we are looking at data both knowing what those crown jewels are; and collecting the data necessary from our fabric of sensors throughout the enterprise to know what is going on around us.

Second, we have ICAM (Identity, Credential, and Access Management) identity which is absolutely core to what we're doing, but there are other elements in identity that we're still looking at building out – especially around non-person entities.

Then we have the trust engine which is an area we are pushing hard. We're looking at the Technology Modernization Fund as a way to take advantage of some of the cool technology that's out there such as AI, AML, Robotic Process Automation; and bring it in from an enterprise perspective across the entire enterprise which is frankly really hard to do. Lots of ZTA solutions out there do have elements of machine learning and AI built into that particular product space or service space. But is it enterprise-wide and can it co-mingle with other things? There are various degrees of capability there.

Finally there is that control fabric, the control plane and that's another area of work for us that we're driving hard; it's probably the most nascent on the horizon for us because we just awarded EIS (Enterprise Infrastructure Solutions) and we're getting lots of incredible technology through that service offering.

Profile Of A ZTA Lifestyle

ZTA is a "lifestyle"; I think I am safe in saying that Zero Trust is the pursuit of perfection; and we will likely never get there, but we're going to pursue the hell out of it until we get as close as we can.

With data, when we look at Zero Trust from the cybersecurity perspective, we knew even a data warehouse was not going to be sufficient for us over the next five, ten years when it comes to ZTA.

So over two years ago we started building a cyber data lake; the whole concept being that we want the native data in its raw format (accurate, thorough and timely) to be in our data lake or accessible by our data lake in a data lake fabric. We've made some good architectural decisions building in the ability to grow, so elasticity is not an issue.

> ZTA is a "lifestyle"; I think I am safe in saying that Zero Trust is the pursuit of perfection; and we will likely never get there, but we're going to pursue the hell out of it until we get as close as we can.

The other part we are looking at how do we then make use of all that data. We are doing some pretty cool stuff with our human skill sets as well; we're bringing on actual data scientists into our security operations space, because they're going to be the ones who are going to help us train the machines later. But first they need an idea of what data we have, what it looks like, where there might be nuances to that data. Then where do we need to build out a data warehouse-like capability?

As we bring on additional Zero Trust capabilities they have to feed into that ecosystem to be able to leverage what's in that ecosystem. We call this our Data Dominance Initiative.

Priorities: SASE and SOAR

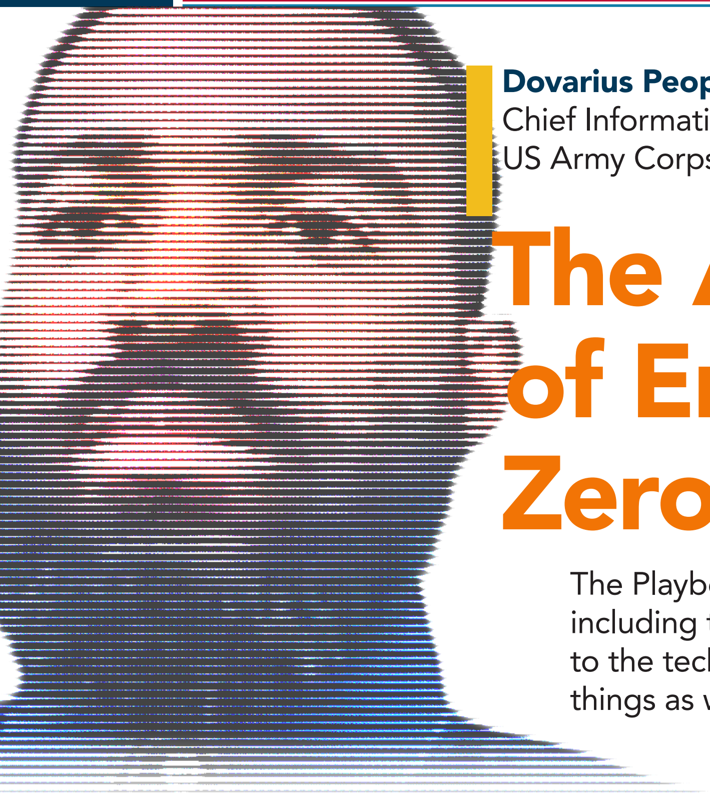
The real opportunity on the horizon is around a Secure Access Service Edge (SASE) and Security Orchestration and Automation Response (SOAR) especially as it relates to our security operation. Combined these two areas make about 90% of ZTA a real possibility.

We're really talking two areas: (1) the idea of the control plane and that's where a lot of that SASE technology comes in. The important part about the SASE technology is how it relates to how we move the Trusted Internet Connection (TIC) into the cloud. Really we're talking about SASE and talking about moving the idea of a tie-cap, which is a physical construct into a virtual concept which is now going be in the cloud. That's just a fundamental game changer. Combine that for example with some the endpoint client technology where the end user is no longer using a VPN they way they think because that client on the endpoint is going to handle almost all the encryption and it's going to be done without their involvement or interaction.

Wow! What a win for the end user and that's really how we start selling Zero Trust as it's not only good for the goose and the gander, it's going to make your job better and easier because a lot of the security interruptions that you feel you may have now they are frankly going to fade away.

On the source side that gets into that trust engine discussion and how do we really start the orchestration and automation of actions starting in the Security Operations Center.

When we talk about SOAR and SASE, those are the capabilities that we are bringing to the forefront; and for us in the next two-three years that's what we are really going to be driving hard on. ■



Dovarius Peoples
Chief Information Officer (CIO)
US Army Corps of Engineers

The Army Corps of Engineers' Zero Trust Playbook

The Playbook playbook goes through 12 different areas including the training aspects from the executive level down to the technician that is responsible for implementing those things as well.

Progress: Zero Trust IT and OT Controls Into Next Generation Firewalls

Things were progressing on Zero Trust before the Executive Order came out. We've already had good conversations with the Federal CIO Council members on Zero Trust and internally in the Department of the Army.

We have developed what we call the Zero Trust Playbook. The Playbook playbook goes through 12 different areas because when most people talk about Zero Trust they only talk about it from about three different perspectives. But we have gone through it from all aspects of Zero Trust to include the training aspects from the executive level down to the technician that is responsible for implementing those things as well.

Mr. Peoples comments are from the Federal Executive Forum on Zero Trust Architecture broadcast on Federal News Network.

Because ultimately in order to implement and execute Zero Trust, you have to be trained and we have put a heavy emphasis on the training of our personnel. Another thing we have done is look at Zero Trust from the perspective of not IT, but operational technology (OT) as well because the Corps has a heavy civil mission and that civil mission includes working with a lot of the levees, locks and dams at the local state level.

We support those state levels when it comes to disaster recovery, waterway missions and critical infrastructure and those type of things. This is one area that we believe could be enhanced with Zero Trust even as we work to meet the Executive Order that was published. So we are looking at this from all aspects – OT, IT – and how do we implement our Zero Trust framework through a playbook and that playbook also constitutes training as well.

Success: From Conceptualization To Operationalization

One of the things we have to do at the Corps is emphasize how we meet the end user where they are. How do we meet that engineer at a distant site enabling them to do their mission effectively and efficiently? Ultimately IT from our perspective is an enabler; so a lot of time we use a lot of technical terms and we talk a lot of technical language, but the end user says "what does this mean to me?"

So we begin to take the conceptual aspects of Zero Trust and begin to operationalize that concept. With

with that being said, from a DOD perspective many are probably aware of the CVR (Commercial Virtual Remote) environment that was just was recently decommissioned due to the fact that we're beginning to modernize and think a little bit differently. But the CVR is a great example of how we operationalize the Zero Trust methodology and concept due to the fact that with Microsoft Teams capability, it enables collaboration or mission collaboration to an end user through a mobile device. That means you can do your job from anywhere effectively and collaborate efficiently with anybody whether that is the Department or in the federal space DOD and non-DOD entities.

Whether you were Air Force, Army, Navy or throughout DOD, you had the ability to connect with all your partners. That means being able to deny all except those allowed by exception; partitioning to allow for those that need access to their mission critical data, mission critical elements; and being able to have good access to view and receive those logs and communicate externally with vendor partners to be able to secure that information as well. So that is a good example of how we operationalize the concept of Zero Trust to enable the end user to effectively be able to perform their mission.

Ultimately being able to access critical information through a mobile device – whether you are sharing it with other mission partners or using it internally – is the goal.

Then again we are also looking at it from the perspective of OT. When you think about construction, being able to build different buildings and you have Wi-Fi sensors and all those other things inside of the enterprise, you have to be able to deploy some Zero Trust principles in order to ensure that those OT capabilities are properly secured as you transfer buildings over to different customers.

So, we have done a lot in that space and continue to lean forward, learn and grow. But we have to begin to execute on the Zero Trust principles and not just theorize conceptually about some of those things as well.

Priority: Continue Our Digital Transformation Journey

We are continuing with that same theme we've had of meeting the end user where they are. But there are several critical priorities that we are beginning to put focus on: one is the leveraging of shared services.

When you talk about Zero Trust you think about shared services and the federal government. That's one of the things I personally believe that from a federal DOD-side of the house, we could do a lot better job of leveraging some of the things our brethren in other organizations have done. And using Zero Trust to ensure that it's properly secure so leveraging that capability to help empower the end user.

In order to be a really world-class organization – which we continue to emphasize in the Corps – that digital transformation journey is very critical and key. Zero Trust is an enabler of mission effectiveness and efficiency; so being able to secure and protect all by leveraging a lot of other good cyber practices such as continuous monitoring and those types of things.

I think last but not least is we're putting a lot of emphasis on the data modernization, data strategy journey. Ultimately being able to access critical information through a mobile device – whether you are sharing it with other mission partners or using it internally – is the goal. Being being able to secure that data through the Zero Trust methodologies and principles allows us to be a lot more efficient when it comes to meeting mission goals and objectives. ■

Paul Morris
Chief Information Security Officer (CISO)
Centers for Disease Control (CDC)

The CDC Rolls Up Its Sleeves

The CDC needs to get data to whoever needs it, where they need it. Moving into a multi-cloud environment where identity and access are monitored through Zero Trust principles, the CDC is moving towards an era where data can move securely between clouds.

Progress: Bringing Identity Access Controls Into Next Generation Firewalls

The CISO Council (Chief Information Security Officer) has been working hard. But to get where we're going takes good policy and takes a lot of people rolling up their sleeves.

There's a lot of existing projects in different places in the enterprise under different teams. So, how do you bring them together so that we can start to think about establishing trust in any user, on any device, when accessing data. And bring those together so that a decision can be made at that point in time whether this is an approved connection.

We're taking advantage of Tech 3.0 opportunities that are available to us with a solution that brings cloud access directly down to the user. That's really an opportunity to use SASE technology and really also provide that tech security monitoring capability that is so important.

Mr. Morris comments are from the Federal Executive Forum on Zero Trust Architecture broadcast on Federal News Network.

The upside to our users is we don't have to back all that data back to our data center up through a single TIC from the department which reduces that latency as we're finding ourselves all in multi-cloud environments. Bringing all those things together is a big plus.

We're also working hard right now on bringing identity access controls into our next generation firewalls. We know – based on the attacks, breaches and ransomware attacks – adversaries are coming in at the application and user level.

So we are thinking about how to use name spaces instead of IP addresses for specific users or groups. That's part of the decision policy point of saying "do they really need access to this data?" Along with network segmentation, we're starting to build that architecture and that framework where I think you are going to see results long term of keeping adversaries out of our networks.

Success: People Only Have Privilege For The Job They Are Doing

I would really have to point to our Privileged Access Management (PAM) efforts. These things work when you have people who understand the complexities of what that means. It brings the elements of separation of duties and privilege which are so are so critical in defending against an adversary. Our program has really advanced past just managing an active directory by installing technology so that when we grant access there is a lot of administrative and technical checks along the way. These make sure that you are granted access to a use case or that you need to have elevated privileges.

So we go through those checks before we grant that. We cycle your credentials – your user name, your password – every time that you use them. We throw them in the trash and then we watch them and make sure those people who are using those elevated privileges are staying where they should be. Are they in the same building that they should be; are they working during the times that they should be; or are they trying to give themselves more privileges?

Those things set off alarm bells that make us all go running and we're constantly looking at Office 365 and Exchange.

So we continue to evolve those capabilities and we're going to continue moving that out to all programs, out to a mobile device and into the cloud. That is so critical for making sure that people only have the privilege they need for the job that they are doing; and then we make sure that doesn't change unless we actually make that change.

We are moving towards an era where we can move data back and forth between clouds, between the premise and the cloud and do that quickly and securely.

Priority: Leverage Zero Trust In A Multi-Cloud Environment

Our number one priority is to support our mission. We are still knee-deep in a response to the pandemic. We've deployed multiple national level critical systems that support the ordering and tracking of vaccines, tracking of testing and then bringing that data from across the nation, whether it's a small public health department at the state level all the way to our data stores. So. how do we quickly make sense of the data?

We're talking about data analytics; we're talking about accessibility and getting that to the people who need it quickly; and making decisions at the national level that go down to the state and local level. So it is a Big Data challenge and an opportunity to add that to what we've also received funds for our specific public health data modernization initiatives, which are allowing us to upgrade legacy systems of data collection supporting all the mission areas of CDC.

We're bringing those to the cloud, we're bringing that data into a data lake and into multiple areas. It gives us an opportunity as we're doing these changes to apply the Zero Trust architectures to the things that we learn. I think the opportunity and priority for us is to make sure that we are leveraging Zero Trust and looking at users as to who has access and then making it easier for our user.

Again we need to get the data to whoever needs it, where they need it. I would say that one of the big things is as we move into these multi-clouds that we can monitor securely and provide access; and we are moving towards an era where we can move data back and forth between clouds, between the premise and the cloud and do that quickly and securely leveraging the technologies that we've talked about by people and applications that are trusted in this framework.

There's a lot of work on policies, but again we need to embrace the future to really take hold of the modernization and innovation that we're undertaking. ■

Kevin Bingham
Zero Trust Technical Lead
Cybersecurity Directorate
National Security Agency (NSA)

At NSA, Helping Customers Get To Zero Trust

The main attribute of a successful Zero Trust program is getting that full buy in from the senior leaders of the organization all the way down to those engineers, the architects, the administrators, the implementers of the capabilities themselves.

Progress: Embracing Paradigm Change

We are trying to continually advance and improve our customer's networks over time. For a decade NSA has had this belief that the "assumed breach model" was really a good one – one that customers needed to take into account. But what we found was that there were a lot of people that just continued to do things the way they had done them in the past. To have the confidence to break away from that legacy mindset of those programs and those activities that you have been doing in the past to do something different and new is hard – even when you accept that an assumed breach model is what you have to go with.

Mr. Bingham comments are from the Federal Executive Forum on Zero Trust Architecture broadcast on Federal News Network.

And two years ago when we started studying how can we get a push for improving the security on the inside of some of our networks, we looked at Zero Trust and thought that it gave a nice disciplined approach to start being able to understand the different pillars of functional capability areas that people needed to start putting attention into. That is what really attracted us to it.

That way we would be able to have a security model encompassing a paradigm change in the way we do things to accept that assumed breach model and actually do some things that are different. We started locking down those privileged accounts and those accesses from the users and the devices to stop the adversary's ability to maneuver through the network. So we are pretty excited it and think that as the adoption of this security model starts to gain momentum and as people start seeing positive results of their work in this space that we'll see not only improvements across the federal and DOD space, but also in the vendor community too to support the needs of their customer base.

Success Improves Using Red Teams For Assessment

My team is externally focused so we're focused on customers. In our effort to learn and help customers get to Zero Trust, we have looked at a number of different examples and we've worked with a number of different partners along the way. As a result, we've seen those efforts that work well and get up to speed quickly and those that don't.

I would say that one of the attributes of a successful Zero Trust program is really getting that full buy in from the senior leaders of the organization all the way down to those engineers, the architects, the administrators, the implementers of the capabilities themselves. When we see that, things roll pretty quickly. When we don't see that, it's not that the organizations don't come around to recognizing the value of Zero Trust but it slows things down a lot. So that's an attribute of a successful program – making sure you have that full support of the organization and buy in. When you get that it's fantastic.

This is a paradigm change so we need to make sure that people aren't just saying "sure I'm doing some Zero Trust and I know that I got to worry about users and devices and whether or not those devices are able to access resources", but accepting that an adversary is assumed in the network you really need to have Zero Trust there in order to drive change. It's not necessary to be paranoid about protecting those privileged accounts; in truth it's the way we should have been doing things for years and the assumed breach model helps us get there. Understanding that paradigm change drive changes within your network.

> This is a paradigm change so we need to make sure that people aren't just saying "sure I'm doing some Zero Trust" and actually take action.

A good mental exercise is to think about the capabilities that you choose. For example, if you're on an open Wi-Fi coffee shop network that you're trying to secure, how would you do that differently? It's not about the technology either, it's about implementation of the capabilities, the implementation of the model itself.

We've seen customers buy new products to drive change and we've seen some military partners do it with very little cost using enterprise software licenses and capabilities successfully. That is fantastic but ultimately the resources need to be both on the people side and the funding side.

Another important factor for success are having the right the methods to do validation right. An example of that could be bringing in a Red Team in so that you have an assessment that has baselined your environment in the past and then be able to measure your effectiveness as you start rolling out Zero Trusts in the future to where you are doing better.

Are you shutting the Red Teams down or are they still able to get around? If they are, then have them help you figure out what changes need to happen in order for you to tighten up that network. We're seeing success out there with a little going a long way; and as people are starting to roll out a properly implemented Zero Trust model, we start seeing success from those Red Team assessments pretty quickly.

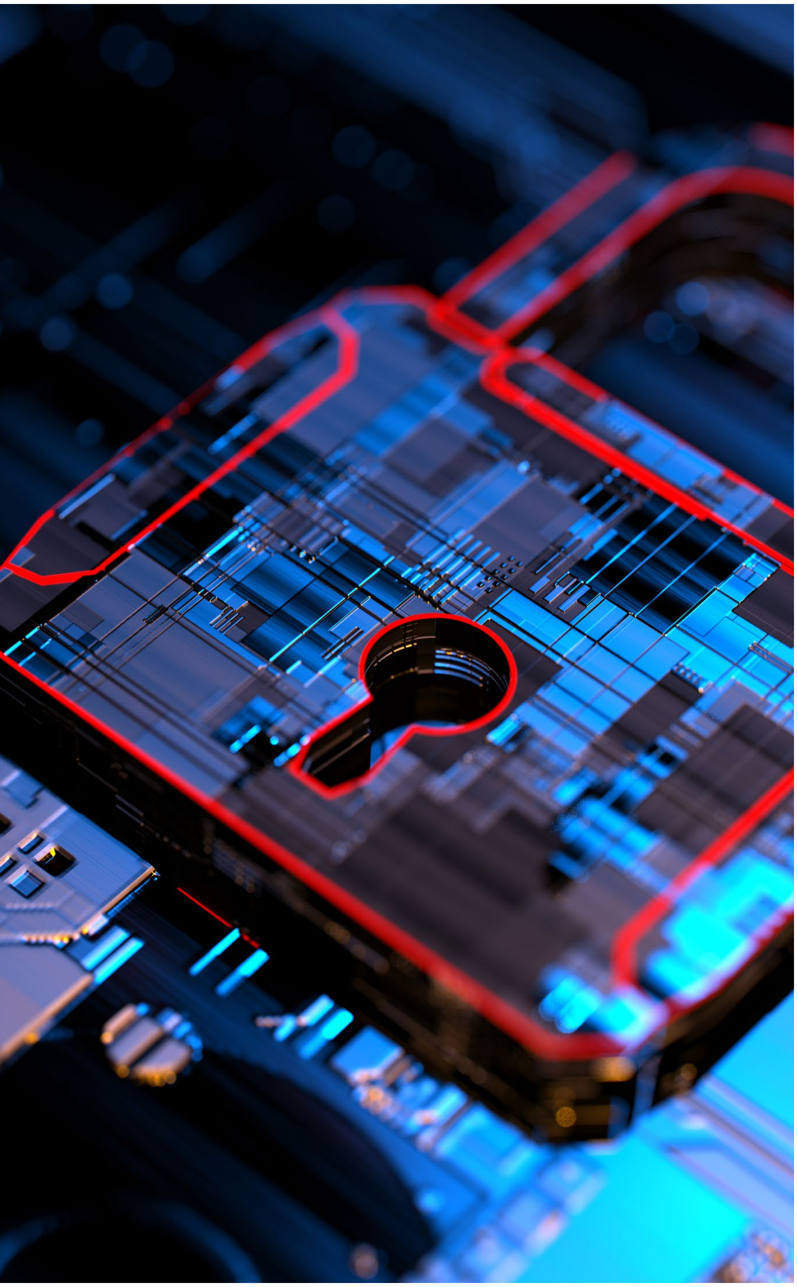
Priority: Create Guidance Documents To Move Towards Zero Trust

My team is externally focused on customers. Our customers are critical system owners including national security systems that include DOD customers as well. We've been working with the Defense Systems Information Agency (DISA) and Cybercom over the last year to try to create guidance documents that will help the DOD specifically to understand and move towards Zero Trust;

So DOD released a Zero Trust reference architecture back a few months ago which we're hoping will help people understand within the DOD how to apply Zero Trust principles. Following from that our team is focused on partnerships with DISA to make sure we understand what test beds we need to continue to develop in order to learn, practice, innovate and turn that into future guidance; and then evolve and learn how to do Zero Trust capabilities more efficiently whatever those challenge areas happen to be.

That might be in data tagging, data protection, identity. Those are challenging areas for us already; but for us it's going to be trying to stay connected with our customers in the community and try to produce the guidance that we feel will help them in areas that may need help. ■

Technology Firms Tackle Zero Trust



Don't Trust: Verify

Implementing Zero Trust involves both implementation of technology, but also a shift in culture and attitude toward cybersecurity.

Don Maclean
Chief Cybersecurity Technologist
DLT

If you haven't suffered a cybersecurity breach, you soon will: That's one of the underlying tenets behind the Zero Trust approach to cybersecurity.

The "moat-and-castle" approach to security does not work. For confirmation, look no further than the recent intrusions affecting our nation's critical infrastructure: Kaseya, the Colonial Pipeline hack, the venerable the Office of Personnel Management (OPM) hack of 2015 and the biggest and most sophisticated of all, the Sunburst intrusion.

John Kindervag coined the term "Zero Trust" while working at Gartner, to describe the phenomena of the disintegrating network perimeter – accelerated by the pandemic – and the associated failure of traditional network-perimeter defenses.

Today, the term arises constantly, but what exactly is Zero Trust? It is a philosophy and set of security principles based on the acknowledgment that we need to re-think security from the ground up. Obviously, this is a tall order, but the advent of cloud computing offers a rare chance to deploy completely new models of information technology as well as security. There are many approaches to Zero Trust; let's look at some of the more common facets of this concept.

Visibility: Data, Traffic and Devices

If you can't see it, you cannot protect it. Data-flow diagrams, Secure Sockets Layer (SSL) decryption, and device management and discovery are all critical aspects of visibility, which underpins all other aspects of security, especially in a Zero Trust environment.

Network Architecture

Kindervag states, "The actual design of a Zero Trust network should be based on how transactions flow across a network and how users and applications access toxic data." This approach applies equally to on-premise network design and cloud architecture. It's a relatively new and different approach to network architecture, and it may take time for technical professionals to learn and implement. Micro-segmentation is a key element here.

Automated Incident Response

If you assume your organization will be breached, automate response to intrusions. Micro-segmentation is essential to this component of the Zero Trust approach.

Zero Trust is a philosophy and set of security principles based on the acknowledgment that we need to re-think security from the ground up. Zero Trust is not a product or specific technology and the advent of cloud computing offers a rare chance to deploy completely new models of information technology as well as security.

Threat Intelligence

Often overlooked, threat intelligence is a key part of a Zero Trust implementation. Threat intelligence lets you anticipate breaches and protect against them in advance. You may not stop every breach, but you will stop some if you stay ahead of the game.

Data Protection

In real estate, the mantra is “location, location, location.” In data protection, it is “encryption, encryption, encryption.” Data is most organizations’ most valuable asset, so encrypt it in place, encrypt it over the wire (even on the “internal” network) and use file integrity monitoring and remote deletion and encryption.

Identity and Access Management (IAM)

A one-time login with user ID (Identity) and password is only the beginning. Multi-factor authentication (MFA) is an important step up, and continuous identification and authorization are really the essential elements of IAM in a Zero Trust context.

Application Security

Application security includes use of secure code, knowing and validating your application inventory, and a solid approach to developing secure applications: DevSecOps. DLT’s Secure Software Factory is an excellent comprehensive approach to creation and maintenance of secure software in any organization.

Zero Trust is a concept and strategy, not a product or specific technology. Implementing Zero Trust involves both implementation of technology, but also a shift in culture and attitude toward cybersecurity. Keep both elements in mind as you pursue your journey into Zero Trust.

DLT has recently launched the Zero Trust Hub to guide public sector agencies through Zero Trust implementation. Access our free resources and tools to better understand Zero Trust from multiple perspectives, and to identify common themes that emerge from the major frameworks and initiatives. Get insights on common challenges and sought-after solutions addressed by the Zero Trust framework.

Learn more at Cybersecurity-Solutions@dlt.com. ■

About The Author

Mr. Maclean, Chief Cybersecurity Technologist with DLT, has extensive experience working with U.S. Federal agencies, having managed security programs for U.S. Department of Justice, U.S. Department of Labor, Federal Aviation Administration, Federal Bureau of Investigation, and U.S. Department of the Treasury. He contributed to the Cybersecurity Solarium Report, whose recommendations appeared in the National Defense Authorization Act (NDAA). He is certified as a Forrester ZTX (Zero Trust eXtended) Strategist and Cybersecurity Maturity Model Certification (CMMC) Registered Practitioner.

Four Actionable Steps for Agencies to Get Started with Zero Trust

A Zero Trust framework moves away from one-time security gating decisions, toward continuous assessment of the risk level of the user and device, and dynamically adapting access privileges based on changes in the risk level.

Tony D'Angelo
Vice President, Public Sector
Lookout

In May 2021, President Joe Biden signed an executive order to strengthen U.S. cybersecurity defenses. The guiding principle is that organizations need to adopt a Zero Trust framework for cybersecurity. You may ask: what exactly am I trusting and what does "zero" have to do with it? Trust in this case is all about whether a user, their device and the network they are using will introduce risks of a cyberattack. These risks could come in many forms – malware or ransomware, vulnerabilities that can be exploited, or compromised credentials or devices. Zero Trust is about "not trusting" the user, device or network connection until you can verify the risk level and understand whether it meets your security requirements.

Without Zero Trust, users are granted privileges to your infrastructure and data once and security teams have limited visibility into what the user or device is doing. Without reverifying the risk level, it is free to access any resources. If a cyberattacker subverts the device or user account, then the attacker can easily move laterally and likely to go undetected, resulting in a breach.

A Zero Trust framework moves away from one-time security gating decisions, toward continuous assessment of the risk level of the user and device, and dynamically adapting access privileges based on changes in the risk level.

As a result, a Zero Trust framework enables agencies to more effectively protect apps and data in the age of telework and cloud collaboration.

The federal government wants to apply modern Zero Trust technology to ensure that employees, data and its infrastructure are protected. Below are four steps you can take right away.

Step 1: Ensure your agency can continuously assess risk on endpoints

With many remote workers using personal devices these days, it's important to ensure that only trusted devices can access your network.

Agency cybersecurity leaders can take steps to ensure that any device – whether it's a smartphone, tablet, Chromebook or PC – will not introduce malware or create a pathway for an attacker to gain access to your infrastructure.

Step 2: Provide dynamic and granular access

Multi-factor authentication is a good first step towards knowing whether an account is compromised, but it's not enough. Agencies also need to be able to

> Government data also should be encrypted wherever it goes — in transit and at rest — whether it is being emailed, uploaded to a cloud or downloaded to a local drive. Only the highest level of encryption is sufficient so that only authorized users with the encryption key can gain access.

spot abnormal behavior that might indicate an internal or external threat. This can be achieved with a cloud access security broker (CASB) solution that has robust user entity and behavior analytics (EUBA). By understanding how employees usually behave, agencies can spot malicious activity and prevent insider threats and advanced attacks.

Step 3: Verify cloud configurations

It's important to verify the security posture of the cloud applications used by government employees. Misconfigurations in software as a service (SaaS) applications, such as Box, or Microsoft 365, and infrastructure as a service (IaaS) like AWS, Azure or GCP environments can create opportunities that cyber attackers exploit.

Agency cybersecurity teams can utilize SaaS Security Posture Management (SSPM) and Cloud Security Posture Management (CSPM) tools to verify cloud security configurations and prevent them from creating opportunities for cyberattackers.

Step 4: Secure data regardless of where it goes

It can be overwhelming to manage the security of cloud applications and the data that flows through them, especially when multiple clouds exist and a myriad of work streams are in play. Agencies need to have full control over their data regardless of how it's handled or where it goes.

To ensure sensitive information does not leak out accidentally or is stolen by a threat actor, organizations have a single viewpoint to see what's happening and manage granular access policies based. This can only happen if there's an understanding of the user or device's risk posture, what they need access to and the types of data and apps required for productivity.

Government data also should be encrypted wherever it goes – in transit and at rest – whether it is being emailed, uploaded to a cloud or downloaded to a local drive. Only the highest level of encryption is sufficient so that only authorized users with the encryption key can gain access.

The Executive Order is a good reminder of the critical need for both the public and private sector to rethink cybersecurity. To deploy Zero Trust and secure mission-critical data, agencies need an integrated security platform that covers the endpoint, the cloud and everywhere in between.

For more information on how Lookout delivers Zero Trust to government, please visit www.lookout.com/gov. ■

About The Author

Mr. D'Angelo leads the Americas Public Sector team at Lookout, bringing more than 30 years of experience in the IT industry. He received his Bachelor of Science in mechanical engineering from the University at Buffalo and has spent his entire professional career in Washington, D.C. Having joined Lookout in 2019 to lead the Americas commercial enterprise team, he now heads the combined federal-SLED business unit.

Contact sales-pubsec@lookout.com for more information or visit www.lookout.com/gov.

Advancing Zero Trust IT with PAM and IAM

Integrating Privileged Access Management (PAM) and Identity Access Management (IAM) is essential to your identity security strategy.

Clarence Hinton
Chief Strategy Officer and Head of Corporate Development
CyberArk

The need for strong Privileged Access Management (PAM) controls has continued to increase as IT teams look to secure what have become highly distributed computing environments due to the pandemic, digital transformation, cloud migration and the shift left.

Not only are end users more likely to be accessing corporate resources from anywhere, but they now expect it, noted Yuval Moss, CyberArk VP Identity Security, in his talk, "What is Identity Security?"

While several years ago only small groups of users (mostly IT admins) were considered privileged, this isn't the case in today's cloud and hybrid environments.

What's more, it's become apparent that each machine – and even individual components of an application – have an identity that needs to be managed. Without the right controls in place, any of these identities can become a privileged identity, opening doors to valuable data and assets.

Similarly, the attacker landscape is evolving. Cyber attackers have increased in number, sophistication and aggression. These factors have combined to lead to an exponential increase in cybersecurity threats facing enterprises across the globe.

A Security-First, Least Privilege View of Identity-Related Risk

Rather than managing PAM and Identity Access Management (IAM) platforms in isolation, CyberArk is making a compelling case for integrating these capabilities via a unified software as a service (SaaS) platform to achieve and maintain Zero Trust security in the most friction-less way possible.

The company, as part of that effort, showed how organizations can apply policies based on identity and least privilege access rules to desktops or even specific end users using either single sign-on (SSO) or biometric tools.

"PAM and IAM are coming together," said Khizar Sultan, Senior Director for Product and Solution Strategy at CyberArk during a "Why Integrating PAM and IAM Is Essential to Your Identity Security Strategy" session. "Identity winds up actually being the new perimeter for security."

CyberArk also stressed the need to protect end users by enabling policies to isolate sessions using a continuous authentication mechanism that makes

CyberArk is making a compelling case for integrating PAM and IAM capabilities via a unified software as a service (SaaS) platform to achieve and maintain Zero Trust security in the most friction-less way possible.

certain end users are active in a session, in addition to protecting them from cyber attacks aimed specifically at browsers. As an extension of that capability, it's critical to enable an audit trail that tracks all actions made during a session.

In general, managing the lifecycle of passwords and privileges based on identity within the context of a task will be crucial. End-users need to be able to assign a higher level of privilege in a just-in-time fashion to complete a specific task, based on their specific identity or the role they play within an organization.

The goal is to enable organizations to implement Zero Trust policies in a way that doesn't jarringly disrupt business process workflows. Naturally, there will also be a need to provide the monitoring tools so that IAM and PAM capabilities are being optimally employed.

Most organizations had already begun to gradually transition toward Zero Trust IT architectures. The COVID-19 pandemic simply accelerated that shift once IT organizations realized many employees would continue to work from anywhere for the long run.

The challenge is finding a way to seamlessly implement Zero Trust principles and capabilities so employees, customers, and business partners won't either reject out of hand or, more likely, waste countless hours trying to find a way to workaround.

Learn more at www.cyberark.com. ■

Michael Vizard, Freelance Writer and Editor at RCF Media, who covers Cybersecurity issues, contributed to this article.

About The Author

Mr. Hinton is Chief Strategy Officer, Head of Corporate Development at CyberArk. He is responsible for formulating, assessing and executing strategic growth initiatives.

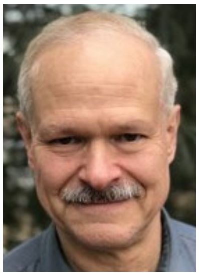
Prior to CyberArk, Hinton served as Senior Vice President of Corporate Development at Nuance Communications, where he was responsible for identifying, developing and executing acquisitions, divestitures, minority investments and joint ventures.

Hinton holds an MBA from Harvard Business School and a Bachelor of Science degree in Engineering with honors from the University of Pennsylvania.

Modernizing Federal Cybersecurity

Organizations should consider using firewall-based Zero Trust because it consolidates and optimizes security operation and management in any environment, whether in the cloud, at the edge, or on-premises.

Jim Richberg
Public Sector Chief Information Security Officer
Fortinet



The United States Federal government is massive and doesn't typically make big changes with great speed, except in extreme situations. The fact that President Biden issued an Executive Order (EO) with specific timelines related to modernizing cybersecurity is an indication of just how critical changing and evolving the federal government's security posture has become.

Recent high-profile cybersecurity breaches like the SolarWinds intrusion have led to the EO, which is a comprehensive plan to better secure federal systems and protect critical infrastructure and data in the United States. Although the EO is focused on Federal systems and services the private sector provides to those networks, this infrastructure includes both public and private systems that are vital to national security and systems, which provide many essential services that underpin American society.

The EO accurately points out that "incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments." But even the most lofty and laudable goals have to be broken down into manageable steps before anything can happen. The old saying about eating an elephant one bite at a time isn't wrong. You have to start somewhere.

Start with Section 3

In the EO, Section 3 addresses modernizing Federal Government cybersecurity and cites a number of areas for improvement. Although the other sections of the EO are certainly important, taking the fundamental steps toward modernization outlined in Section 3 first can help move forward with progress on the requirements listed in the other sections as well.

At a high level, Section 3 of the EO states that agencies should accelerate migration to cloud technology, implement a Zero Trust architecture, improve cloud security, multifactor authentication and data encryption, centralize and streamline access to cybersecurity data to drive analytics, and improve communication and training.

Zero Trust Architecture

In Section 3, it states that agencies must move to a Zero Trust approach to security by implementing strong authentication capabilities, network access control technologies, and application access controls. Zero Trust Network Access (ZTNA) entails

Zero Trust verifies and authenticates user and device identify before every application session to confirm that they meet the organization’s policy to access that application, and grants the least privilege necessary to perform the task at hand.

controlling access to applications. ZTNA verifies and authenticates user and device identify before every application session to confirm that they meet the organization’s policy to access that application, and grants the least privilege necessary to perform the task at hand. A key element of the ZTNA concept is that access is independent of the location of the user. Users on the network should not enjoy any more trust than users who are located outside of the network perimeter or even working off the network. With ZTNA, the application access policy and verification process are the same in all cases.

Organizations should consider using firewall-based ZTNA because it consolidates and optimizes security operation and management in any environment, whether in the cloud, at the edge, or on-premises. This approach makes it possible to enforce a consistent access policy no matter where users, data, and computing resources may be located.

Modernization Needs to Happen Now

Meeting the requirements laid out in the EO isn’t going to be easy, but it needs to happen. The best time to have modernized cybersecurity would have been years ago. The next best time is now. There’s no time to waste because cyberattacks are becoming more aggressive and more damaging every day. Hackers certainly aren’t delaying their activities and neither should we.

Learn more at www.fortinet.com/solutions/industries/government/federal. ■

About The Author

Mr. Richberg’s role as a Fortinet CISO leverages his 30+ years’ experience leading and driving innovation in cybersecurity, threat intelligence, and cyber strategy & policy for the U.S. Government and international partners.

Prior to joining Fortinet, he served as the National Intelligence Manager for Cyber, the senior Federal Executive focused on cyber intelligence within the $80B+/100,000 employee U.S. Intelligence Community (IC). He led the creation and implementation of cyber strategy for the 17 departments and agencies of the IC, set integrated priorities on cyber threat, and served as Senior Advisor to the Director of National Intelligence (DNI) on cyber issues.

Prioritize and Execute: Getting DOD to Zero Trust Faster

Data, applications and workloads represent some of the most critical pieces of our nation's network, but they are often the least protected.

Mark Sincevich
Federal Director
Illumio

If federal defense leaders needed proof of national cyber insecurity, the exponential growth of cyber threats, including the SolarWinds breach and Colonial Pipeline ransomware attack, stand as bold reminders of the need for a cyber overhaul.

Attention is turning to Zero Trust strategies with the recent Executive Order on cybersecurity as a catalyst for security momentum. The Defense Information Systems Agency's (DISA) "Zero Trust Reference Architecture" that embeds security throughout the architecture, instead of only at the perimeter, bolsters this momentum.

President Joe Biden's 2022 budget request to Congress also includes $10.4 billion for Department of Defense cybersecurity, including Zero Trust efforts. Now, DOD agencies and commands must prioritize the components of Zero Trust that will deliver the most immediate security impact.

Prioritizing Mission-critical Assets

Federal leadership has been trying to tackle several aspects of Zero Trust at once, spending a tremendous amount of time on other Zero Trust pillars, such as ICAM (identity, credential, and access management), devices and network security. While each is an important part of an overall Zero Trust architecture strategy, they will not protect the DOD's high-value assets if an attacker is already inside the network.

Dave McKeown, Deputy CIO for cybersecurity and the DOD's Chief Information Security Officer (CISO) explained that we have long understood that an increasingly determined adversary will eventually find a way to breach our perimeter and layer defenses.

Therefore, we must assume the adversary is already on our network and deny by default by assuming compromise.

Data, applications and workloads represent some of the most critical pieces of our nation's network, but they are often the least protected. The National Security Agency's (NSA) report "Embracing a Zero Trust Security Model" directs agencies to shift their security philosophy and to architect security from the inside out to guard mission-critical assets like applications and workloads with Zero Trust segmentation (also known as micro-segmentation).

When a workload is properly segmented, it can appear cloaked or invisible to an attacker. It is crucial that defense agencies prioritize this pillar and execute the strategy by starting with a single critical application or a small number of workloads. This will help them keep their high-priority data secure, even after a breach happens.

Breaches will inevitably occur; the key is doubling down on protecting mission-critical assets like applications and workloads to stop the lateral movement of a cyber attack so agencies and commands can continue to focus on the mission.

When a workload is properly segmented,
it can appear cloaked or invisible to an attacker.
It is crucial that defense agencies prioritize this pillar
and execute the strategy by starting with a single critical
application or a small number of workloads.
This will help them keep their high-priority data secure,
even after a breach happens.

Zero Trust Segmentation For An Immediate Security Impact

To properly secure defense environments, teams must identify their critical applications and workloads, often found in the data center, on the cloud or in hybrid environments. It is essential they create visibility into how applications and workloads connect to one another. After all, they can't secure what they can't see.

Visibility will allow teams to react quickly to threats and changes in workflow. They can then architect their security from the inside out, as the NSA directs, by applying and enforcing Zero Trust segmentation.

Zero Trust segmentation is decoupled from the network, allowing teams to lock down and separate key assets at the speed of the mission. The NSA advises agencies to focus first on protecting critical assets and then securing all paths to access them.

Zero Trust segmentation policies use allow lists that indicate which applications and workloads are permitted to connect. If a connection is not explicitly stated, it is denied by default. This fortifies the network to ensure attacks cannot spread. Zero Trust segmentation blocks unnecessary movement automatically, which keeps critical assets secure.

Defend Forward With Zero Trust Architecture

When it comes to cyber attacks, if agencies need to chase the enemy, sharing threat intelligence, then the damage is already done. Agencies must defend forward with Zero Trust segmentation to not only minimize the spread of attacks but also prevent future cyber catastrophes.

As the DOD prioritizes the Applications and Workloads pillar as the most important piece of their Zero Trust strategy, they will see an immediate security impact. This approach will dramatically reduce the application attack vector by protecting critical applications and workloads even while agencies continue to improve the network.

And as Mr. McKeown said about Zero Trust Architecture: Our networks will be exceedingly more secure, the war fighting mission will be defended, and our adversaries will have to dedicate significant resources only to achieve very small gains.

Learn more at www.illumio.com. ■

About The Author

Mr. Sincevich has more than 30 years experience helping IT firms serve the Federal marketplace. He joined Illumio where he started the Federal and Federal System Integrator (FSI) Business from scratch. Illumio is a cybersecurity software company that enables Zero Trust Segmentation in Defensive Cyberspace Operations. The company helps agencies, commands and organizations achieve Zero Trust and prevent attacker lateral movement by (i) providing real-time visibility, (ii) reducing the dynamic attack surface, and (iii) enabling faster implementation all through host-based micro-segmentation. Illumio is FIPS 140-2 validated, is on the DHS CDM APL and is NIAP Common Criteria Protection Profile Certified. Illumio can be placed in multi-vendor hardware environments, using existing infrastructure to improve agencies' cybersecurity postures and effectively accomplish their missions.

Executive Order on Improving the Nation's Cybersecurity — Ushering in a New Age of Security

This Executive Order makes clear that modernizing our current digital situation is a moral imperative and that failure is not an option.

Sean Frazier
Federal CSO
Okta

President Biden took a major step forward in ensuring that the U.S. government has the resources and focus needed to address our cybersecurity needs with the issuance of Executive Order on Improving the Nation's Cybersecurity. This focus is long overdue. For nearly a decade, we've lived in this tenuous world where the next critical cyber event lies just around the corner, but the seeds were planted long before that.

The day we decided to connect our agencies or our enterprises to the larger network (the Internet), the risks became significantly higher. And now, more than ever, we see attacks like with Solarwinds come along and realize that this is not the end but really only the beginning. We find ourselves wondering if we'll ever be truly safe from attackers in this modern, very digital, very connected world.

Well, it finally looks like, from a government perspective, we are starting down the right path. This EO—which promotes Zero Trust, enhanced endpoint protection, multi-factor authentication, and software development standards—will serve as the initiation of a long-needed shot-in-the-arm for focusing our attention on the ever-increasing threat. It has placed much-needed awareness and focus on true threat mitigation.

Let's face it: we've made it too easy on the attackers. They keep hitting targets with the same tried and true methods of attack (phishing, credential-based attacks, etc.), and yet in the press and in our lives, we tend to spend time talking about "zero-day" attacks and attacks that are novel and sophisticated.

Novel and sophisticated attacks cost time and energy for attackers. But think of our adversaries as business folk, running a business. Why would they focus on very expensive, very limited attack vectors when they have a low-cost, high-success-rate alternative? It doesn't matter what their motivations are—whether financial or political. If they can "do more with less," why wouldn't they? If they could gather and use valid credentials to leverage a valid-looking access flow, that's the path of least resistance. Their business is just like yours; if they see a path with a better ROI, they will certainly pursue it.

This new directive makes clear that modernizing our current digital situation is a moral imperative and that failure is not an option. It also makes it clear that digital modernization or transformation most often takes the form of cloud adoption or the adoption of cloud services to deliver capability.

Many folks out in the world, myself included, have been preaching the benefits of adopting a Zero Trust "mindset" for some time now. This mindset includes providing protections for the most vulnerable attack

Many are advocating the benefits of adopting a Zero Trust "mindset". This mindset includes providing protections for the most vulnerable attack surface (the password) by building systems that utilize Single Sign-on (SSO) and strong Multi-factor Authentication (MFA).

surface (the password) by building systems that utilize Single Sign-on (SSO) and strong Multi-factor Authentication (MFA).

For too long, we've put much of the security burden on the end-user (passwords) without giving them the proper protections for these arcane constructs. This EO shines a light on this oversight and requires us to do better.

The EO also brings cloud modernization into the right area and delivers it through the FedRAMP program, which makes total sense. The FedRAMP program was designed specifically to reduce and manage risk (heck, it's in the name!) and to enable modernized, cloud-based services to become the vehicle for change that most of us knew it could be.

One of the historical problems with the FedRAMP program, while very popular and very successful, is it also becoming a bit of a bottleneck because of its success and popularity. Now that we are thinking about cloud and cloud security as top priorities, the FedRAMP program needs its own funding stream and needs to be a first-class delivery program.

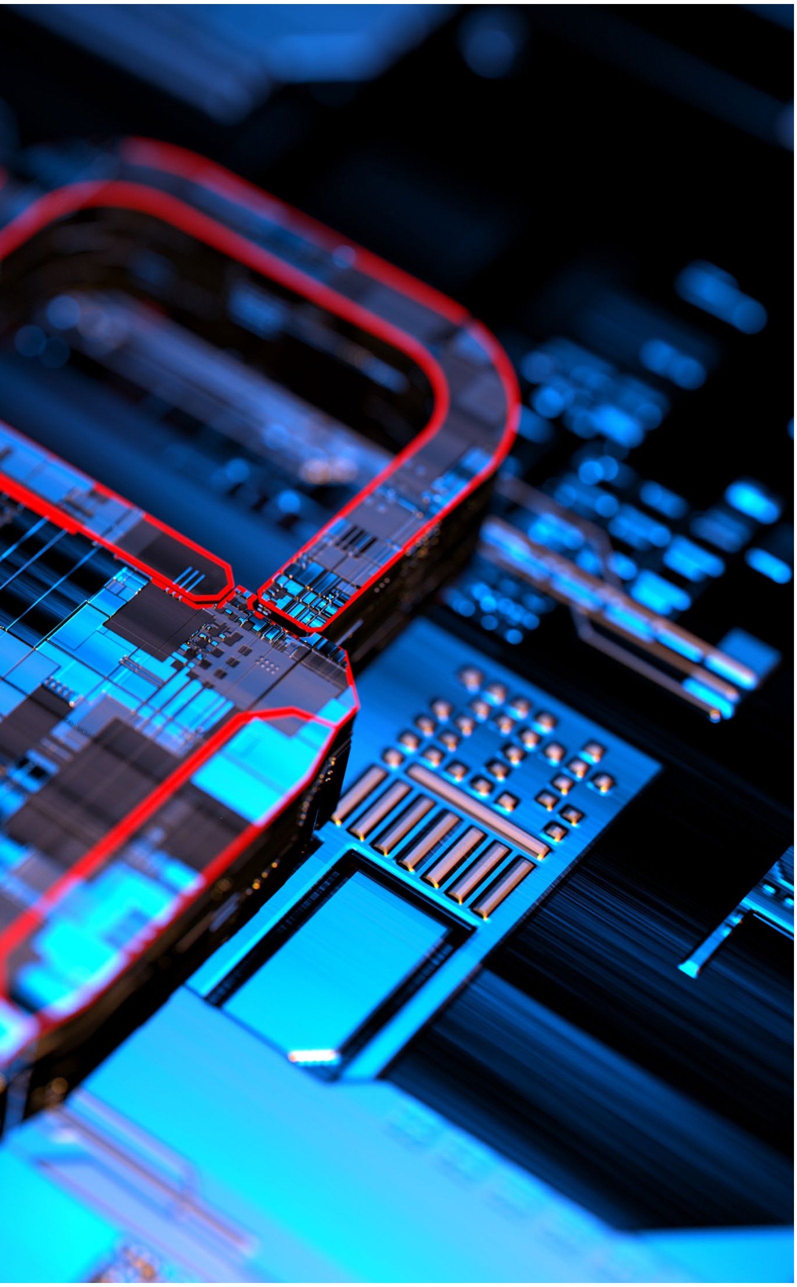
Congress has sought to address this through legislation via HR 21: the FedRAMP Authorization Act of 2021, which was the very first bill passed by the 117th Congress. Enacting this legislation into law, combined with what's required by the executive order, provides a foundation to do cloud security the right way. Now, we just need to match the investment with the promise.

Learn more at www.okta.com. ■

About The Author

Mr. Frazier is Federal CSO at Okta. In his role, Sean acts as the voice of the CSO for Okta's federal business. Prior to joining Okta, Sean spent more than 25 years working in technology and public sector security for companies such as Duo Security, Netscape, Loud-Cloud/Opsware, Proofpoint, Cisco & MobileIron. Sean has helped lead numerous projects used by the Department of Defense and Intelligence Community, including the Fortezza Crypto Card, Defense Messaging System (DMS) and many others. He also has extensive experience in identity and public key infrastructure (PKI), network, applications, mobile and IoT. Sean has testified in front of the U.S. Senate Homeland Security and Government Affairs Committee on the importance of public/private partnership in protecting the nation's digital infrastructure. Sean also advises public/private partnership working groups including ACT-IAC, ATARC and many others.

Former Senior Federal IT Executives Present Pragmatic ZTA Solutions



ZTA's Not A Thing, Not A Widget, ZTA Is A Framework…

Use NIST SP 800-207 as your guiding North Star to implement your own Zero Trust Architecture (ZTA) capability within your own environment.

By **Luke McCormack**
CIO (Retired)
Department of Homeland Security (DHS)

The most important element of Zero Trust is architecture. It's important to say Zero Trust Architecture – it's not a thing, it's not a widget, it's a framework.

ZTA is an architecture that allows you to trust nothing and assume that somewhere inside your network apparatus you have been compromised. You always have to assume that there is no implicit trust granted to anyone under any circumstances; and you need to continue validate that and re-validate that.

In layman's terms: While I am granting you authority to come into my environment and get access to X, Y or Z, the next time you come in I don't just say "hey there you are" and let you in and again give you access to various pieces of information. I am validating you are the "approved person", but I am also validating that the approved person still has the authority to the information and I am doing that in real time, all the time.

ZTA – Where To Start?

I think that is very important to put together a structure, an architecture that allows for that capability. That's not a simple thing to do. You don't buy a box, a piece of software and implement it into your environment and all of a sudden you have this capability. There's a lot of pieces and parts that have to come together to adhere to this architecture to allow those types of things to happen, do it in a real time basis and do it with a level of maturity that you are looking for.

I think a lot of the CIOs struggle with "where do I start"? First you have to baseline your environment and based on that you can understand where you are at, what pieces of technology do you have available to begin to have this capability. And you may have to buy some new software and hardware to enable some of this and then you go through a multi-step process to harden the environment and keep it there.

Google has implemented this capability and it took them 7 to 8 years to fully implement this. So even though they had endless engineering and financial resources to make this happen, it took time. But it gives the community a chance to take the lessons learned from them including some of the products to engineer, design, implement and harden and simply reuse that.

So if you look at Google as a company, they went through this Zero Trust Architecture journey over a long period of time. It took them several years to get there but now the community at large can benefit from that capability.

It's a bit of an arms race; you need a constant flow of funds because you need to change the culture; you have to train people; you have to implement and reconfigure constantly pulling out old technology and putting in new technology.

Funding Critical

To guide the community, OMB has given some directions in the May 2021 Executive Order on Cybersecurity that states agencies will put a plan together and then execute on those plans. I also think this will get the funding.

Nine cabinet level agencies were compromised in the Solar Winds attack and all of them are going to get increased funding for cyber to build out their capabilities and harden their environment that is going to be based on this ZTA.

This is a lifestyle culture change. You need upper level management buy-in along with addtional annual funding. This is a down payment and it's not just to buy products and services; this is a plus up to not only start you on this journey but to keep you on the journey in the years ahead.

That way you don't run into technology that will become outdated and you are able to keep up with current technology; there are a lot of bad actors and you are going to need to refresh and update your architecture to stay ahead of and counter them.

End Users Benefit

The end user gets affected in a positive way. No longer will they have to use a VPN. As ZTA gets more mature and implemented, the whole login process becomes a cleaner and more secure experience because it becomes more embedded and fused into this architecture. Users get to enjoy the seamless capabilities that come along with this – less burden and a better experience.

The same thing goes for machine to machine communications. For example, a bank when it doesn't recognize the computer you are on asks for more proof of identity. They can validate the characteristics, elements of the device and if OK, you can go into the environment. Validation of both the person and the device they are using happens at the same time. ■

About The Author

Mr. McCormack is National Director of ACT-IAC. He also serves as the National Director for the U.S. Cyber Challenge.

Mr. McCormack retired as the Chief Information Officer (CIO) at the Department of Homeland Security (DHS), where he provided strategic direction, cyber security services, oversight to cross-component information technology efforts and IT Cloud/infrastructure services. He also served as the Vice Chairman of the Federal CIO Council. Prior to this appointment, he served as the Department of Justice Deputy Assistant Attorney General for Information Resources Management/Chief Information. .

The ZTA Education Challenge

Zero Trust is really kind of the nuts and bolts needed to move out of the old way of doing business into a new way that helps keep us secure in the future.

Charlie Armstrong
CIO (retired)
Customs and Border Protection (CBP)
Department of Homeland Security (DHS)

With the implementation of a Zero Trust Architecture (ZTA), organizations are moving away from a site-based perimeter security approach, moving towards a software defined perimeter approach. This is key because – especially with Covid – you have a workforce working from home or working from anywhere so you absolutely need to extend security far beyond what we used to call the perimeter.

Everybody is migrating to cloud services – not just a service but multiple services. Agencies are hooking up to a variety of different Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) capabilities, so Zero Trust is really kind of the nuts and bolts needed to move out of the old way of doing business into a new way that helps keep us secure in the future.

Further, because it's more policy-based, it requires a lot more upfront thought not just from the security types, but from the leadership as to what the policies should be and who has access to what. This is more than just getting into the system itself, but what access, what data, what devices is approved for that user.

This will help make security more ubiquitous in the future, so if a bad guy gets in, at least the agency can limit what intruders get access. This is opposed to "I'm in and now I get to go everywhere across the network, both horizontally and vertically". Also ZTA helps contain internal threats; that can be someone who wants to do something bad or someone who accidentally does something that disrupts, not meaning to. ZTA will help us to get to a very different state of trust.

Lifestyle Changes

We are always changing what we do and how we do it; that requires us to think before we make changes as to what does the security need to look like around us. That's something we haven't done in the past.

For me, the challenge for the CISO community is educating people across agencies and across user communities as to what does ZTA mean to them. That is both in terms of how they may need to operate differently or think about things. They need to make sure they are moving forward in lock-step with the security policies and administrative needs in their agency. That way there won't be surprises that either slow down the mission from getting new things done

ZTA is more policy-based and requires a lot more upfront thought not just from the security types, but from leadership as well. This is more than just getting into the system itself, but what access, what data, what devices is approved for that user.

versus losing or compromising security in order to get there.

The education challenge has always been there, but even more so in this Zero Trust environment.

That's because there is no clean slate. There are no agencies being stood up from scratch. So if you look across the federal, state and local landscape, you already have a lot of existing infrastructure and systems that are out there. And everybody has the goal of migrating to the cloud, using more SaaS offerings, maybe owning and operating less equipment and relying more on commercially available services.

The issue is how do you make all that fit together and make it so you can plug and play and move faster. This sets up a framework to move quicker, but move more methodically in terms of thinking about those things that impact access and who should get to do what.

ZTA should also cause leadership to examine who gets exemptions. For years, we have allowed executives and people with special privileges to do things that they didn't need to do or shouldn't be doing inside the network.

This causes problems because the adversaries get access because someone left a door open or because someone doesn't want to use multi-factor authentication or doesn't want to follow the policies in place for everybody else.

As a result, leadership will be more conscious because there will be more accountability and it will be their necks are on the line if this stuff doesn't work. ■

About The Author

During his career at DHS, **Mr. Armstrong** functional responsibilities included software development, infrastructure services and support, tactical communications, the laboratory system and research and development functions, and IT modernization initiatives supporting CBP's core business processes.

He also served as DHS Deputy CIO where he was a champion of the Department's IT initiatives for improving the agency's secure information sharing capabilities through the consolidation of infrastructure and strengthened security. Mr. Armstrong has over 30 years of leadership and technology experience in the operations and management of IT.

Zero Trust Implementation Lessons Learned

Zero Trust is simultaneously a concept, a framework, an approach, an architecture, a set of guiding principles, a systems design, and an operational model to cybersecurity and risk management.

Joseph Klimavicz
Managing Director
KPMG LLP

Today, every government agency is completely dependent on digital technology to perform its mission, and everyone is counting on Zero Trust to secure this technology and associated data to ensure citizen services and national security. The Executive Order (EO) 14028 on Improving the Nation's Cybersecurity (May 12, 2021) emphasized Zero Trust, but what are some of the big lessons learned implementing Zero Trust?

Zero Trust is simultaneously a concept, a framework, an approach, an architecture, a set of guiding principles, a systems design, and an operational model to cybersecurity and risk management that safeguards the environment no matter where data and people reside to build the capability to trust nothing and verify everything.

This broad definition of success means some government agencies may have already claimed victory, but in my federal service experiences as well as recent experiences supporting federal clients, the reality is a few government agencies have limited Zero Trust implementations. Sharing Zero Trust lessons learned from these early implementations will be critical to broader rollout across the federal landscape.

With Zero Trust, the user's identity, their devices, the software, the network, or the data could be compromised, and agencies need to implement Zero Trust controls across these six foundational elements: identities, devices, applications, data, infrastructure, and networks.

This approach ensures that identities are verified and authenticated and that devices are compliant before granting access to any resources. Visibility and analytics, along with automation, need to be applied continually and comprehensively. Zero Trust implementations requires significant integration of third-party applications, but agencies can leverage key cyber services from the big cloud service providers to streamline implementation.

Zero Trust may seem like a lot to take on, however, the use of existing technologies and revamping of current processes and strategies can allow agencies to implement a new approach to cybersecurity without huge capital investments. Government agencies may already have many of the components in place providing many of the alerts and analysis needed for Zero Trust. For example, existing Identity, Cre-

With Zero Trust, the user's identity, their devices, the software, the network, or the data could be compromised, and agencies need to implement Zero Trust controls across these six foundational elements: identities, devices, applications, data, infrastructure, and networks.

dential, and Access Management (ICAM), Security Information and Event Management (SIEM), and Continuous Diagnostics and Mitigation (CDM) tools may already be providing many of the alerts and analysis needed for Zero Trust. The SIEM delivers intelligent security analytics and threat intelligence across the enterprise and provides a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Agencies will also need to incorporate threat intelligence feeds, network and system activity logs, identity management systems, data access policies, and a policy engine. These are all important Zero Trust components. Access to resources will need to be determined by policy and consider the requesting system as well as observable user identity and behavioral traits, and the threat environment. The policy administrator, with its security orchestration automated response solution, acts upon alerts to initiate actions to disconnect offending systems and deny prohibited access to resources. Agencies will need to implement a trusted and secure communications platform between edge devices and services in the cloud or on-premises. A private multi-segment and multi-path blockchain is ideal to securely hold cipher keys and this can be used to enforce the use of enterprise public key infrastructure (PKI).

Thinking about the future, Zero Trust solutions will need to evolve. Quantum computing may be able to crack today's encryption, and artificial intelligence (AI)-powered cyber-attacks may occur. We will certainly need to incorporate AI into Zero Trust implementations and establish a resilient cyber ecosystem through connected technologies like AI. We may need to think about broader implementation of Host Identity Protocol (HIP), or implementation of Blockchain to treat the network as a massive ledger. And we will need continued close cooperation between government and industry. ■

About The Author

Mr. Klimavicz is a Managing Director with KPMG LLP where he leads the government Chief Information Officer (CIO) advisory practice and helps government clients develop and implement digital transformations. Mr. Klimavicz's 37-year career in the federal government began with the Central Intelligence Agency (CIA) as a scientist and culminated with the U.S. Department of Justice (DOJ) as Deputy Assistant Attorney General and CIO from May 2014 until March 2020. Mr. Klimavicz also served as National Oceanic and Atmospheric Administration (NOAA) CIO and Director, High Performance Computing and Communications from 2007 until 2014, and as the National Geospatial-Intelligence Agency Deputy CIO from 2003 to 2007. In 2012, Mr. Klimavicz received the U.S. Presidential Rank Award for Distinguished Executive Service, and he is a CIO-SAGE at the Partnership for Public Service.

Accelerating Mission Outcomes through Zero Trust

David M. Wennergren
CEO, American Council for Technology & Industry Advisory Council (ACT-IAC)

"Only trust thyself, and another shall not betray thee." William Penn. As John C. Maxwell pointed out, "progress does not occur without change," and change inevitably brings both opportunity and risk. One of the top risks we currently face is the ever-increasing threats to our networks and data. Go to any news source and the headlines trumpet the headaches that technology leaders face daily–Solar Winds, Colonial Pipeline, ransomware, phishing attacks–the list goes on and on. William Penn may have spoken a truth about trust, but it does seem to be a negative view for us at a time when collaboration and information sharing is a key to success in both business and government. Indeed, as a technology leader, if we follow Penn's quote to its logical conclusion, we may be inclined to so lock down access to our networks and systems to prevent malware from taking root, that we also impede the flow of knowledge in to and out of our organization–in a sense, we create a self-inflicted denial of service attack. Fortunately, there is another path.

"Trust is the glue of life." Stephen R. Covey. Zero Trust has generated a lot of interest recently as a key tool in reducing cybersecurity risks while still enabling information sharing and legitimate access. In the old world of on-premise enclaves, a network perimeter-based protection scheme was a logical choice. However, as we moved into a cloud-based, mobile access, virtual work environment world, it became crucial to shift away from a security strategy that may have made initial access hard, but once gained, allowed unfettered access to everything within a network.

Zero Trust uses a combination of robust identity management, access control, data-level security and strong monitoring to create an environment where positive identification and authorization allow transactions to occur–enabling access to trusted entities while simultaneously preventing access by untrusted individuals.

A couple of years ago, the U.S. Federal CIO Council asked the American Council for Technology and Industry Advisory Council (ACT-IAC) to evaluate the maturity and availability of Zero Trust for federal agency adoption. The government and industry volunteers at ACT-IAC responded with two reports.

The first report, *Zero Trust Cybersecurity Current Trends* identified foundational concepts, strategies, and challenges. Key findings included:

- Zero Trust adoption does not require a wholesale replacement of existing networks or a massive acquisition of new systems, and many organizations already have in place some of the building blocks for Zero Trust.
- Zero Trust solutions are available and in use in the private sector.
- Zero Trust efforts require a combination of poli-

Zero Trust principles not only help to reduce cybersecurity risks, but also help to ensure that we accelerate, rather than impede, the legitimate flow of knowledge.

cies, practices, and technologies to succeed.

- Organizations should have a solid handle on their people, assets, data and associated business processes to implement Zero Trust.
- Many cybersecurity professionals endorse Zero Trust as an effective approach to strengthen protection against current threats.
- Success at Zero Trust does require a "whole of agency" effort and commitment from both the technology team and mission owners.

The second report, *Zero Trust Report: Lessons Learned from Vendor and Partner Research*, highlighted available products, solutions and use cases, all aligned with National Institute of Standards and Technology (NIST) standards and Department of Homeland Security guidance—a reminder that you're not alone, and that there are new products, repurposed existing products and a number of "lessons learned" that you can take advantage of in deploying Zero Trust. Both reports are available at www.actiac.org.

"Love all, trust a few, do wrong to none." William Shakespeare. Cybersecurity remains a national imperative, with the intellectual capital and competitive advantage of our Nation at stake. As we replace aging legacy infrastructure and systems, it is crucial that we embed cybersecurity tools and best practices from the start, rather than as an afterthought. It's also crucial that as we emerge from the pandemic, we ensure that we don't just observe the changes we've faced, but instead learn from them. Recognizing that the changing way we do business demands new cybersecurity approaches, Zero Trust principles not only help to reduce cybersecurity risks, but also help to ensure that we accelerate, rather than impede, the legitimate flow of knowledge, both within our organization and with our customers and mission partners. ■

About The Author

Mr. Wennergren is the CEO of ACT-IAC, the national non-profit public-private partnership dedicated to advancing the business of government through the application of technology. He has extensive leadership experience in information technology and change management and has served in a number of senior positions, most recently in the private sector as a Managing Director at Deloitte Consulting LLP, EVP & COO at the Professional Services Council and a VP at CACI International Inc., and prior to that in government as Department of the Navy CIO, Vice Chair of the Federal CIO Council, DoD Deputy Assistant Secretary of Defense/Deputy CIO and DoD Assistant Deputy Chief Management Officer. He is also a fellow and chair of the board at the National Academy of Public Administration.

Zero Trust Is Critical for Managing Your Organization's Network Security

Zero Trust security models hold the promise of vastly enhanced data protection and governance for those organizations willing to adopt a few key principles.

William J. Bender
Chief Information Officer, U.S. Air Force (retired)
Senior Vice President
Leidos

An overarching premise of this viewpoint is that your network is under attack at this very moment and that adoption of a Zero Trust framework can harden your environment against such attacks while minimizing the impacts to your network once compromised.

Digital Transformation is ushering in an increase in malware attacks, IoT exposures and data breaches, because it has become both easier to phish users on mobile devices and to take advantage of poorly maintained Internet-connected devices. Workforce mobility and hybrid IT models have placed most workloads beyond the shelter of on premise networks and traditional perimeter defenses, leading to significant user access and data concerns.

With an ever-increasing number of sophisticated cybersecurity attacks on federal agencies, IT leaders and decision makers are prioritizing Zero Trust Security Architecture to protect their data. While Zero Trust implementations are moving beyond mere concepts, however, there remains a significant divergence of thought among cybersecurity professionals in applying Zero Trust principles. On one hand, the sheer volume of cyberattacks and enormity of data breaches challenge confidence levels in any organization's ability to defend themselves, while on the other confusion reigns as to how and where to implement Zero Trust controls in every organization's uniquely-hybrid IT environment.

Still, Zero Trust security models hold the promise of vastly enhanced data protection and governance for those organizations willing to adopt a few key principles:

- A shift in cybersecurity mindset accepting that a network is already breached (or will be soon)
- A reduction in implicit trust of authenticated users
- An architecture designed to specifically reduce damage caused by attacks
- A prescribed set of incremental steps to improve defenses against advanced cyber threats

Some organizations hesitate to implement Zero Trust because they have legacy applications that could delay or prevent cloud deployment. Others

Applying a Zero Trust model that aligns to hybrid IT migration can allow organizations to reap the benefits of compute and store economies, while also experiencing a non-disruptive implementation toward Zero Trust functionality.

see themselves having greater data protection obligations, and are averse to having controls and other sensitive information leaving their premises, or may have already made significant investments in data center infrastructure.

Having acknowledged threats exist both inside and outside traditional network boundaries, however, Zero Trust architectures serve to keep the focus on desired business outcomes centered on maintaining user productivity while defending the network from those threats. Applying a Zero Trust model that aligns to hybrid IT migration can allow organizations to reap the benefits of compute and store economies, while also experiencing a non-disruptive implementation toward Zero Trust functionality.

Conceptually, Zero Trust architectures eliminate implicit trust in any one element, node or service by requiring continuous verification of the operational environment via real-time information from multiple sources to determine access and other system responses, while also focusing on protecting data in real-time within a dynamic threat environment. To achieve this requires comprehensive security monitoring, granular, risk-based access controls and overall security system automation.

Again, committing your organization to a Zero Trust strategy requires a cultural mindset shift from multi-layered perimeter network defenses to an acknowledgement your network has already been breached. Hence, the primary objective changes to minimizing the impact. Zero Trust, done right, implements a comprehensive set of mitigation protocols including software-defined perimeters, micro-segmentation for more granular identity and access management controls and a series of identity aware proxy controls via continuous authentication and user-based access.

In the end, Zero Trust requires commitment to an adaptive defense strategy and sustainable threat protection as the best way to secure and protect the data that matters most to your organization. ■

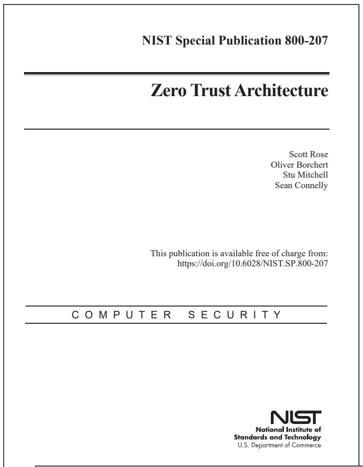
About The Author

Lt. General Bender (retired) most recently served as CIO for the Air Force, where he was responsible for 50,000 cyber operations and support personnel across the globe with oversight for the USAF's IT investment strategy and a portfolio valued at $17 billion. After retiring from the Air Force following a 34-year career there, Lt. General Bender joined Leidos in September 2017. Now tasked with overseeing and managing the Strategic Account Executives, a group of customer-facing senior-level former government officials, Lt. General Bender aims to bolster customer relationships and advance strategic initiatives to foster organic growth.

NIST Talks Zero Trust

Continued from page 9

to zero trust. There is also an email address on the NCCoE project page that can be used to send feedback to the project team. This address as well as information about the community of interest are both listed on the NCCoE ZTA project page.



NIST Special Publication 800-207

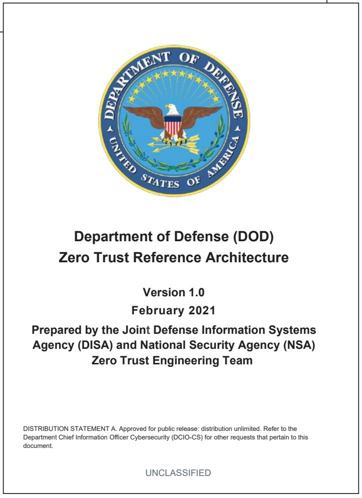
Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



Department of Defense (DOD)
Zero Trust Reference Architecture

Version 1.0

February 2021

Prepared by the Joint Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited. Refer to the Department Chief Information Officer Cybersecurity (DCIO-CS) for other requests that pertain to this document.

UNCLASSIFIED

Q. *We understand NIST's core and functional components of Zero Trust. How would you assess the state of the art in terms of where each component stands today? Which components are more advanced and which ones need more development in order to achieve the desired capabilities?*

A. Scott Rose: Of all the functional components described in NIST SP 800-207, the policy engine component will likely see the greatest advancement in functionality. As Zero Trust sees wider deployment and experience, we anticipate improvements in how the policy engine uses information about the organization and environment to make access request decisions. We are also seeing the start of how machine learning and artificial intelligence can be applied to the work of the policy engine and how these technologies can be used to automate cybersecurity policy checks, enforcement, and responses. As technology advances, the policy engine may become a partner to the human administrators of the organization's infrastructure more than just a tool used to operate the infrastructure.

We also may see new standards or protocols for the communication between functional components. One of the concerns we frequently heard from agencies was the risk of vendor "lock-in" based on a specific technology. There was the desire for a more "open" Zero Trust based on an open set of standards that would allow policy engines, policy administrators and policy enforcement points from different vendors to work together in a single solution or as a federated deployment in a coalition. This is not possible with a single protocol but will likely be some sort of framework using various standards that would allow for interoperability between components and between components and information feeds (e.g., logs, threat intelligence, etc.). ■

ON THE FrontLines MAGAZINE

TREZZA Media Group
Connecting Partners Through Mindshare Media

Public Sector COMMUNICATIONS

Publisher
Tom Trezza Jr.
President
Trezza Media Group
3101-So. Ocean Drive Unit 1803
Hollywood, Fl. 33019
ttrezza@trezzamediagroup.com
201-757-7405

Editor
Jeff Erlichman
Managing Partner
Public Sector Communications
Louisville, CO
djerlichman@comcast.net

Art Direction
Reuter & Associates, bill@reuter.net

U.S. Cyber Challenge Awards Program And Cybersecurity Summit

October 6, 2021
a virtual event

REGISTER TODAY

act-iac
Accelerating Government