Toward a Zero Trust Architecture

A Guided Approach for a Complex and Hybrid World

CLOUD SECURITY ALLIANCE OFFICIAL CHAPTER

D.C. Chapter

CSA

CSA cloud security alliance®

Abstract

Enterprise stakeholders must consider the challenges of increased real-time system complexity, the need for new cybersecurity policy, and the strong cultural support that is required to securely operate systems in a complex and hybrid world. Emerging technology solutions and approaches such as Zero Trust are critical to meeting the mandates in United States President Biden's Executive Order 14028, *Improving the Nation's Cybersecurity*. The implications of an emerging, rich, and diverse solutions landscape and the challenges to an organization's ability to ultimately deliver a Zero Trust architecture (ZTA) are explored in this paper. Recommendations are discussed for how industry can improve collaboration among key stakeholder groups to accelerate both enterprise leaders' and security practitioners' adoption of Zero Trust into their environments.

A Product of the Cloud Security Alliance – Washington DC Chapter (CSA-DC) Research Committee
Research Committee Chair: Mari Spina

Acknowledgments

Authors:

Juanita Koilpillai
Jyoti Wadhwa
Dr. Allen Harper
Salil Parikh
Paul Deakin
Vivian Tero
Greg Bateman
Aubrey Merchant-Dest
Jay Kelley
Phyllis Thomas
Uma Rajagopal
Rebecca Choynowski

Contributors:

Jason Keplinger
Tom Stilwell
Lauren Bogoshian
Bob Klannukarn
Joe Klein
Daniele Catteddu
Nirenj George
Jagan Kolli
Andres Ruz

Special Thanks:

Bowen Close

About the CSA DC Chapter

This document was created by the DC chapter of the Cloud Security Alliance (CSA). The DC Chapter of the CSA consists of volunteers who have been at the forefront of cloud security. Visit our website at https://www.cloudsecurityalliance-dc.org/ for more information.

Dedication

This paper is dedicated to Juanita Koilpillai, whose sudden and unexpected death marked a great loss for the cybersecurity community and her CSA-DC Chapter friends. Juanita was a primary author and contributor to this paper and the CSA-DC Chapter working group that produced it. Juanita's contributions to cybersecurity will continue in her stead, strengthening the cybersecurity posture of organizations around the world. Her technical leadership and development of Software-Defined Perimeter (SDP) technologies formed the early foundations of Zero Trust architectures (ZTAs). Juanita was a true light that shone brightly across the cybersecurity community. It is with great sadness we bid farewell to a truly great leader and engineer.

Anil Karmel
President, CSA-DC Chapter

Table of Contents

1 Background

Due to the COVID pandemic, organizations have had to quickly adapt to supporting a global remote workforce. The expansion of remote work and the adoption of cloud technologies have extended the definition of the security perimeter, necessitating adoption of a Zero Trust (ZT) strategy to secure the future of work. Combined with the ongoing shift to more agile and scalable multi-cloud, hybrid architectures, these forces have accelerated more than ever before the need to improve the security and risk management of information systems. IT organizations are now being driven to prioritize their focus on defining and adopting a Zero Trust architecture (ZTA) unique to its environment. The adoption of a ZTA is further promoted by the recent Presidential Executive Order mandating improvements to the nation's cybersecurity[1] and the Federal Zero Trust Strategy.[2]

With perimeter-based and defense-in-depth approaches giving way to this newer security paradigm, enterprises are seeking to reduce security risks, especially as they begin to adopt modern microservice, microsegmentation, and software-defined architectures that enable remote productivity. Although there is broad support from IT vendors, the reality of ZTA is still an ambitious future target state because organizations are just beginning to formulate baselines for their ZTA approach and the industry is seeking insights to form best practices or standards through ongoing collaborations.

This paper will help inform cybersecurity practitioners, engineers, architects, business leaders, and IT stakeholders. Although broadly useful, this paper focuses on a U.S. government perspective. As a result, a general familiarity with NIST SP 800-207 is implied.

1.1 Why Zero Trust?

The ZT model of information security was introduced by the Jericho Project in 2003, recognizing the security challenges of traditional perimeter networking, followed in 2009 (publicly available in 2014) by Google's Beyond Corp project—their implementation of ZT—and then by Forrester Research in 2010. The ZT model "eliminates the idea of a trusted network" and teaches that "in Zero Trust (ZT), all network traffic is untrusted. Thus, security professionals must verify and secure all resources, limit and strictly enforce access control, and inspect and log all network traffic."[3] In 2019, NIST authored a Special Publication on Zero Trust Architecture[4] (SP 800-207) that melds ZT ideas into an abstract definition of ZTA and presents guiding tenets for development and implementation of

[1] Exec. Order No. 14208, 86 FR 26633 (May 12, 2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[2] U.S. Office of Management and Budget. (n.d.). *Federal Zero Trust Strategy. Cybersecurity & Infrastructure Security Agency*. Retrieved September 29, 2021, from https://zerotrust.cyber.gov/federal-zero-trust-strategy/

[3] Kindervag, J. (2010, September 17). *No More Chewy Centers: Introducing the Zero Trust Model of Information Security*. Palo Alto Networks. https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

[4] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August 11). SP 800–207, Zero Trust Architecture. NIST. https://csrc.nist.gov/publications/detail/sp/800-207/final

ZTA; illustrated in Figure 1. Industry dynamics driving the adoption of a new ZT security landscape include exploding security cost, broad use of 5G, cloud computing, the Internet of Things (IoT), and microservice-oriented architectures. These factors contribute to redefining ownership boundaries and usage patterns by diminishing the prominence of fixed physical or software-defined network boundaries.

Zero Trust Tenets from NIST

1 All data sources and computing services are "resources"

2 Communications are secured regardless of location

3 Access to individual resources is granted on a per-session basis

4 Access to resources is determined by dynamic policy and other behavioral and environmental attributes

5 Integrity and security posture of owned and associated assets is monitored and measured

6 Dynamic resource authentication and authorization are strictly enforced before access is allowed

7 Information on current state of asset, network infrastructure, and communications is collected to improve security posture

Figure 1. Zero Trust Tenets, NIST SP 800-207

As organizations continue to migrate all or parts of their network to the cloud, stakeholders at government agencies and commercial enterprises must secure their private, public, or community cloud instances in a new way. Although the need is imminent, this change in the security landscape will take time and intention to implement. Organizations will need to advance their ability to secure their systems in the cloud with new technology stacks, skill sets, and processes. This presents a challenge of developing new security governance and policies that are based on continuous verification, microsegmentation, software-defined networks, and continuous monitoring and visibility. Implementing and enforcing these modernized policies will require industry players to design and operate a complex mix of both traditional and modern access control and network technologies, customized to their own environment over time.

Commonly deployed approaches, such as always-on VPN connections and routing all traffic through enterprise gateways, have become less efficient or no longer viable from a cost and user experience perspective. Furthermore, much of cybersecurity is based on a signature-based concept, whereby tools look for "signatures" of known bad behavior, but by definition a zero-day threat does not have a known signature. This limitation is addressed by ZT, since ZTAs do not rely on signature- or anomaly-based technologies to help reduce risk. With ZT, security controls are pervasive and rightly trending closer to the actual data and functions, wherever and whenever they are instantiated. However, given the disparity in the rate and level of modernization among organizations, the speed and maturity of industry guidance on how to secure these modern architectures has fallen behind and is at best too uncoordinated for optimal protection of systems and their data.

Maturity for ZT solutions and roadmaps is just beginning, given architecture and marketplace complexity. For example, security practitioners are challenged with identifying users and implementing automated detection of new cyber threats in real-time, multi-cloud environments. Given today's sophisticated and hybrid landscape, this paper proposes foundational elements of a Zero Trust Architecture Capability Maturity Model (ZTA-CMM) and is associated with a ZT roadmap. Ongoing government and industry dialog and collaboration will aid in the development of ZTA-CMM best practices to assess how ZT principles are applied to current architectures and the corresponding ZT roadmap that addresses the gaps, yielding improved risk management and cyber resiliency.

1.2 Assessing the Current Zero Trust Maturity Level

An organization must understand the current maturity level of its ZTA, engaging in organization-wide reviews to conduct a thorough and efficient analysis. This analysis should account for the current people, processes, and technologies in place that contribute to the ZT pillars. Though focused on federal agencies, the CISA Federal Zero Trust Strategy[5] document can operate as a guide for understanding the processes and technologies that are vital for a successful ZTA implementation. Conceptual models and frameworks are being identified by the National Institute of Standards and Technology (NIST) and industry stakeholders[6] such as ACT-IAC[7] and Forrester,[8] and will continue to evolve; however, it should be noted that at this time there is no effort to bring these frameworks together. CISA has released a ZT CMM[9] composed of the following pillars: identity, devices, networks, applications workloads, and data. Together, these five components provide a holistic perspective on the different areas where an organization can apply resources towards the development of its ZTA.

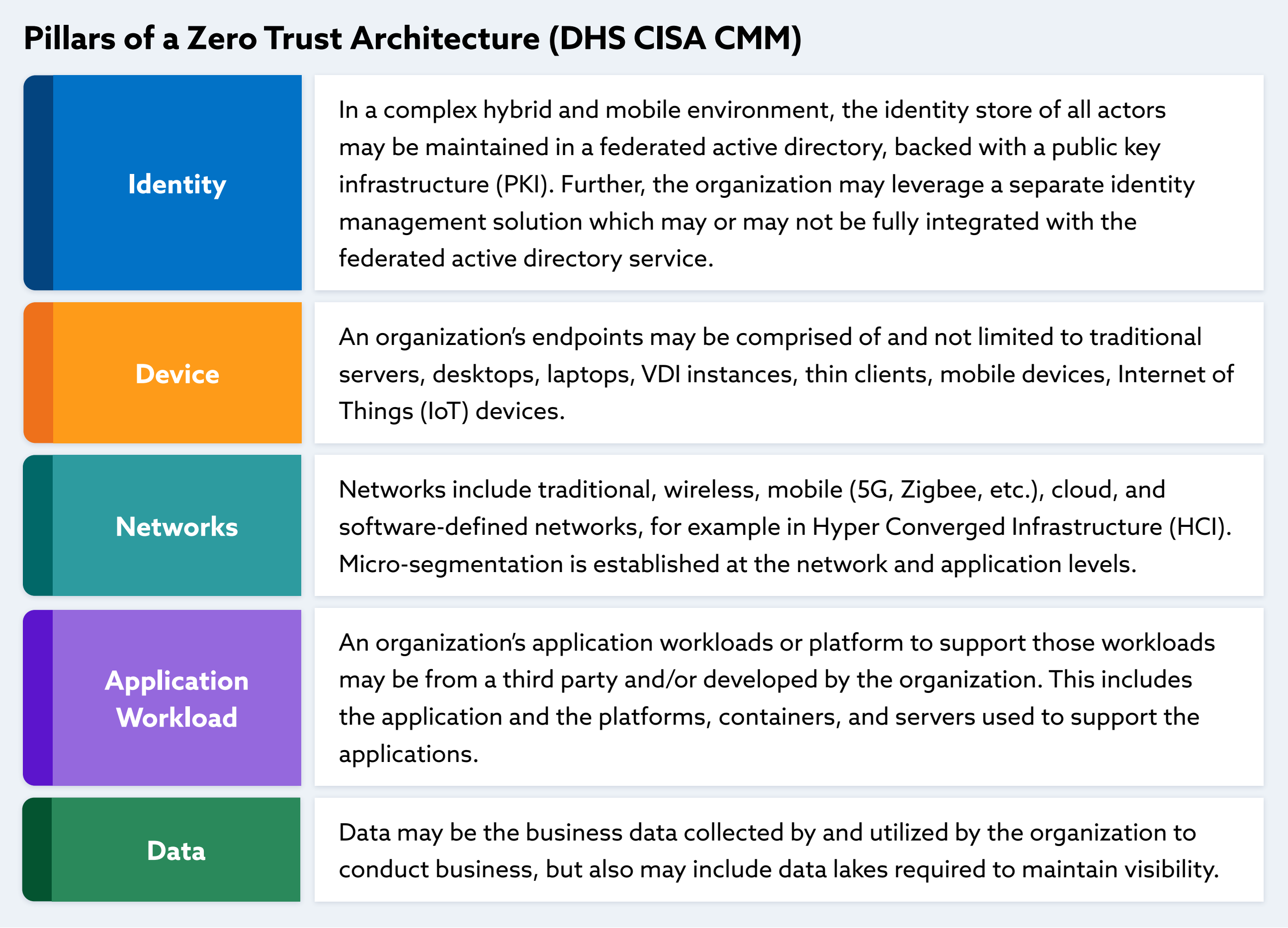
[5] U.S. Office of Management and Budget. (n.d.). *Federal Zero Trust Strategy.* Cybersecurity & Infrastructure Security Agency. Retrieved September 29, 2021, from https://zerotrust.cyber.gov/federal-zero-trust-strategy/

[6] Microsoft. (n.d.). *Zero Trust Model - Modern Security Architecture.* Retrieved September 29, 2021, from https://www.microsoft.com/en-us/security/business/zero-trust

[7] American Council for Technology-Industry Advisory Council. (2019, April 18). *Zero Trust Cybersecurity Current Trends.* https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf

[8] Forrester. (n.d.). *The Zero Trust Security Playbook For 2021.* Retrieved September 29, 2021, from https://www.forrester.com/playbook/The+Zero+Trust+Security+Playbook+For+2020/-/E-PLA300

[9] Cybersecurity and Infrastructure Security Agency, Cybersecurity Division. (2021, June). *Zero Trust Maturity Model - Pre-decisional Draft, Version 1.0.* Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf



Pillars of a Zero Trust Architecture (DHS CISA CMM)

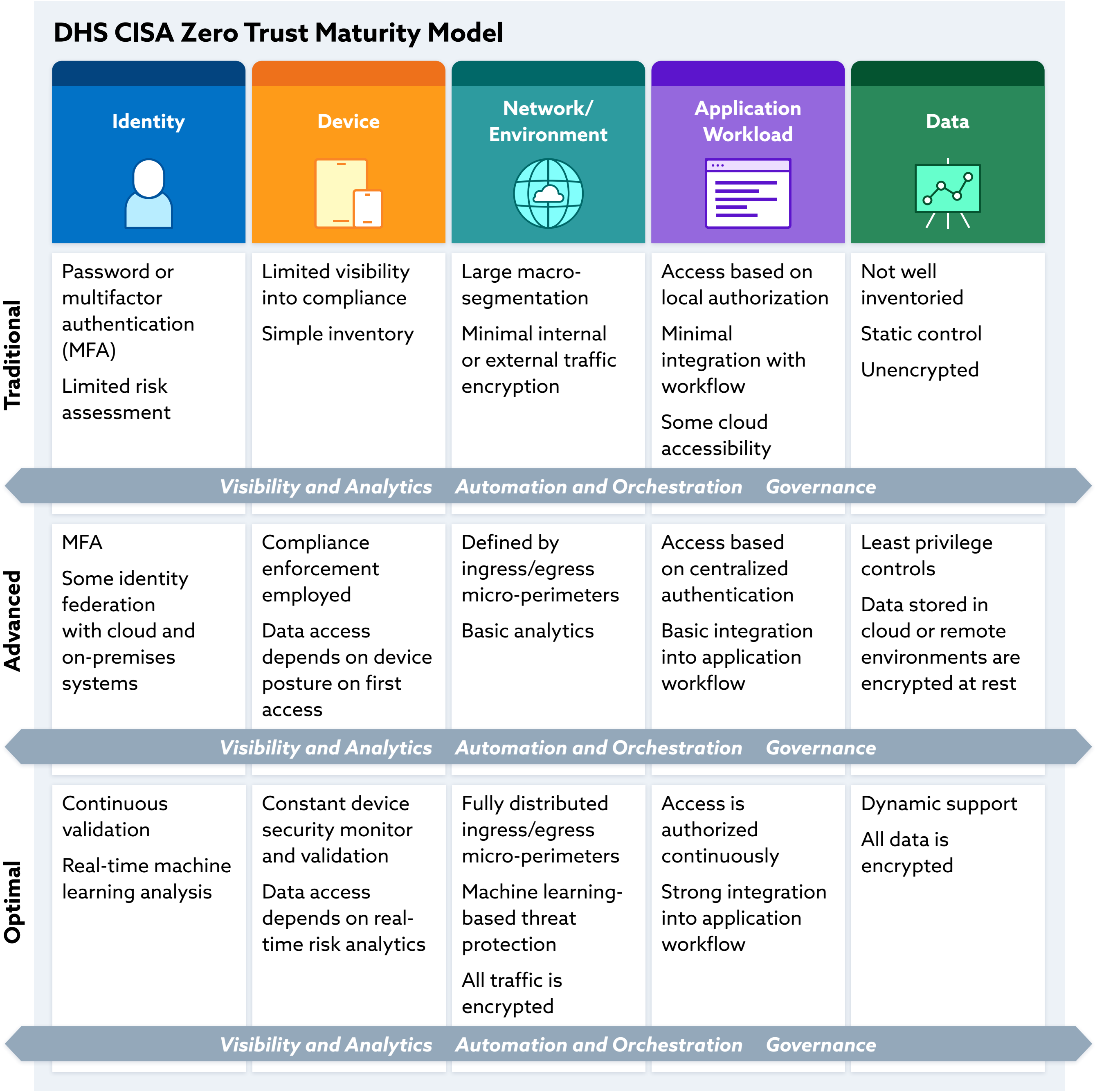
Identity	In a complex hybrid and mobile environment, the identity store of all actors may be maintained in a federated active directory, backed with a public key infrastructure (PKI). Further, the organization may leverage a separate identity management solution which may or may not be fully integrated with the federated active directory service.
Device	An organization's endpoints may be comprised of and not limited to traditional servers, desktops, laptops, VDI instances, thin clients, mobile devices, Internet of Things (IoT) devices.
Networks	Networks include traditional, wireless, mobile (5G, Zigbee, etc.), cloud, and software-defined networks, for example in Hyper Converged Infrastructure (HCI). Micro-segmentation is established at the network and application levels.
Application Workload	An organization's application workloads or platform to support those workloads may be from a third party and/or developed by the organization. This includes the application and the platforms, containers, and servers used to support the applications.
Data	Data may be the business data collected by and utilized by the organization to conduct business, but also may include data lakes required to maintain visibility.

Figure 2. Zero Trust Pillars, DHS CISA ZT-CMM

A ZTA-CMM provides insights into the maturity level of each pillar (shown in Figure 2). Gaining a deep understanding of each area helps to inform organizational stakeholders about their environment's unique strengths and gaps regarding the adoption of a ZTA. Currently, organizations are limited in leveraging a widely accepted ZT maturity model for ZTA assessments, which is a gap in industry guidance and an area that will likely stimulate industry collaboration on the rankings and levels of the ZTA-CMM. In the interim, individual organizations will likely move forward with initial assessments and the results of those first assessments will become the baseline assessment of the organization.

1.3 Developing a Zero Trust Roadmap

As organizations gain more insight into the current state of their ZTA maturity level, they can identify and incorporate into their architecture new solutions that address the gaps and advance their maturity. For example, the DHS CISA ZT CMM (DHS CISA) uses three levels: traditional, advanced, and optimal, as shown in Figure 3.



DHS CISA Zero Trust Maturity Model

	Identity	Device	Network/ Environment	Application Workload	Data
Traditional	Password or multifactor authentication (MFA) Limited risk assessment	Limited visibility into compliance Simple inventory	Large macro-segmentation Minimal internal or external traffic encryption	Access based on local authorization Minimal integration with workflow Some cloud accessibility	Not well inventoried Static control Unencrypted
	Visibility and Analytics	Automation and Orchestration	Governance		
Advanced	MFA Some identity federation with cloud and on-premises systems	Compliance enforcement employed Data access depends on device posture on first access	Defined by ingress/egress micro-perimeters Basic analytics	Access based on centralized authentication Basic integration into application workflow	Least privilege controls Data stored in cloud or remote environments are encrypted at rest
	Visibility and Analytics	Automation and Orchestration	Governance		
Optimal	Continuous validation Real-time machine learning analysis	Constant device security monitor and validation Data access depends on real-time risk analytics	Fully distributed ingress/egress micro-perimeters Machine learning-based threat protection All traffic is encrypted	Access is authorized continuously Strong integration into application workflow	Dynamic support All data is encrypted
	Visibility and Analytics	Automation and Orchestration	Governance		

Figure 3. CISA ZT-CMM, (DHS CISA)

Achieving the targeted maturity level is supported by evaluating the organization's current maturity level and prompting stakeholders to use that evaluation to identify priority areas for execution, resource requirements, and budget allocation over a defined timeline to achieve the targeted maturity level. Targeted maturity levels in advanced environments that already reflect a high degree of ZT approaches in their architecture will be much higher relative to organizations that are starting their security and IT modernization journey. To address the requirements of a ZTA roadmap, stakeholders will need to gain a better understanding of an evolving technology landscape representing modern opportunities to attain targeted maturity levels.

This begins with completing a maturity assessment of the organization's capabilities across each of the five pillars. For each pillar, several questions may be developed so that relevant stakeholders provide a holistic assessment of the level of maturity in each focus area. These questions would increase in the degree of difficulty and scope to result in a more mature aspect of ZT in that pillar. After completing the questionnaire, the organization may leverage the quantified results as a baseline assessment of the organization's current ZTA maturity. Maturity level can be measured and quantified using an organization's rubric, similar to the approach suggest by the CMMC[10] and represented in a spider diagram, as notionally illustrated in Figure 4, alongside a desired or target state of ZT maturity for the organization.

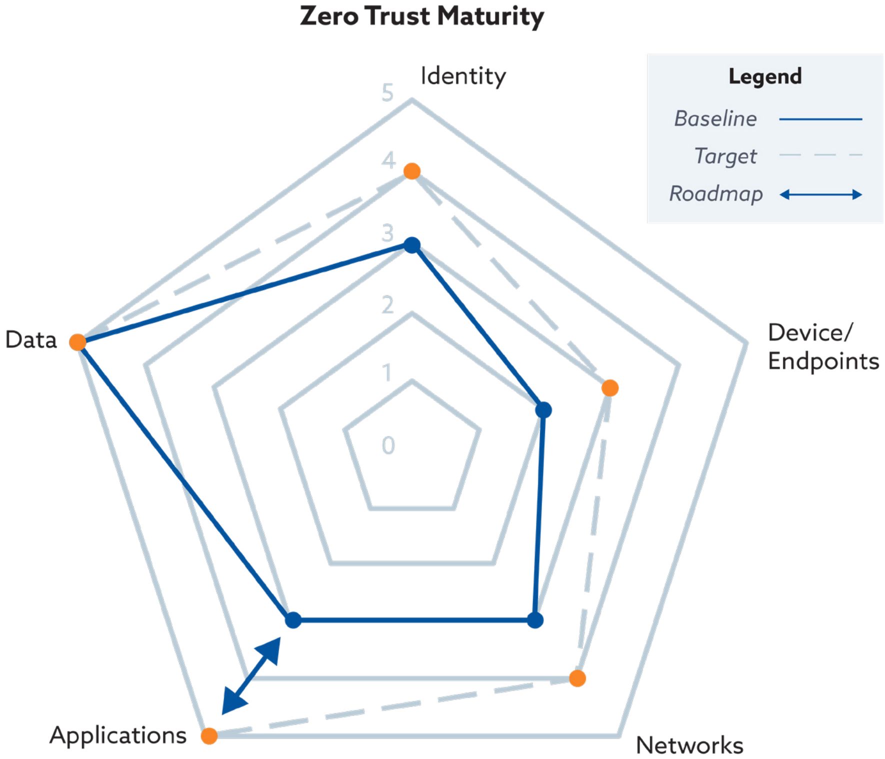


Figure 4. Zero Trust Maturity Spider Diagram (notional)

The resulting differential in the baseline and target points is the gap assessment. The gap assessment includes specific areas for each pillar that the ZT Roadmap will address to methodically and gradually improve the current state to the target state over one to three years.

[10] CMMC Information Institute. (2021, August 21). *DoD/NIST SP 800-171 Basic Self Assessment Scoring Template*. https://cmmcinfo.org/cmmc-info-tools/dod-nist-sp-800-171-basic-self-assessment-scoring-template/

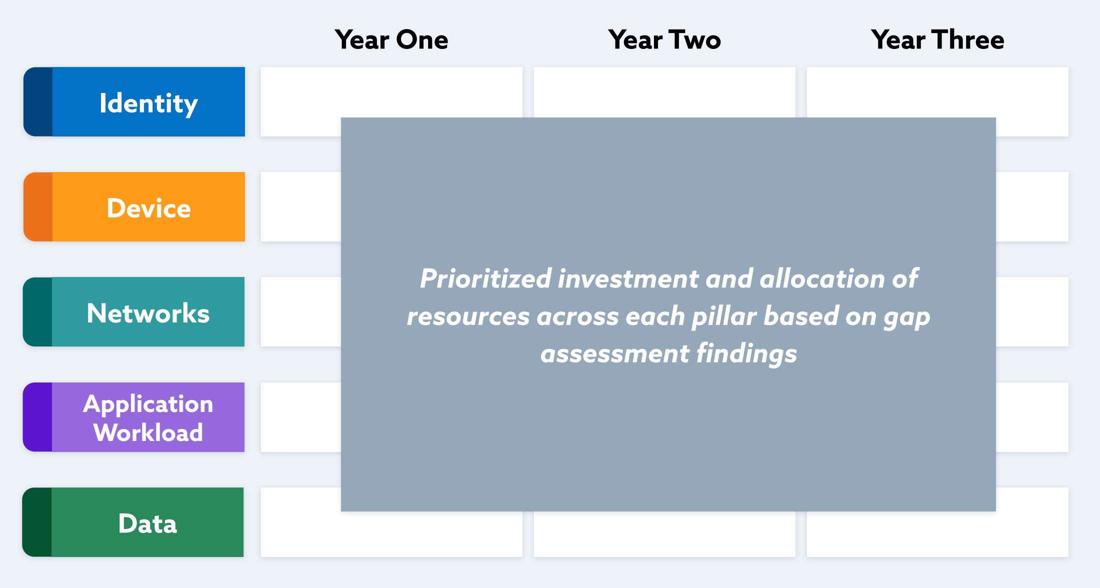

Year One
Year Two
Year Three
Identity
Device
Networks
Application Workload
Data
Prioritized investment and allocation of resources across each pillar based on gap assessment findings

Figure 5. ZT Prioritized Investment Roadmap (notional)

This approach yields a ZT prioritized investment roadmap, as suggested in Figure 5. It should incorporate the use of industry best practices and frameworks, such as the NIST Special Publication (SP) 800 series, CSA Cloud Controls Matrix (CCM), or government Security Technical Implementation Guides (STIGs), as they pertain to each pillar. This will help guide organizations on the detailed process and technology requirements that are missing from their current state in order to achieve their desired maturity level over one to three years. This approach is presented as an example of what is possible and it may be customized for each organization. Future working groups and organizations may develop a standard set of prescriptive questions and graphics describing capability maturity levels for a holistic approach to adopting a ZTA.

2 Considerations for Zero Trust Adoption

In addition to ZT maturity assessment and roadmap considerations, the following four factors are important considerations to developing a ZTA: technology, organizational culture, policy, and regulatory requirements. These internal and external factors influence an organization's ability to understand, design, and implement a ZTA roadmap for today's complex and hybrid environments. They help stakeholders identify which variables are significant barriers or accelerators in their current maturity level of ZTA and which ones most help to advance their ZTA journey.

One essential step in ZTA adoption will be the inventory of people, process technology, critical assets, and security controls. This is key to adopting the architecture successfully. NIST recommends that you start with a single process and continue the organization journey in the deployment of the architecture.

Organizations should target quick wins and understand that adoption of a ZTA is a longer-term, strategic initiative. As such, it requires executive support and ongoing consideration of all these factors over three to five years. A capability maturity model can guide an organization through a journey to understand existing and legacy capabilities while suggesting appropriate questions to ask and seek answers to. For example, questions could address:

> 1. What are the legacy technologies used by the organization?
> 2. What type of data/services are they using?
> 3. What are the specific cloud services implemented?
> 4. Is there a cloud access security broker solution implemented?
> 5. How are identities managed and what tools are implemented ?
> 6. In which phase of the cloud adoption journey is the organization?

However, questions should be tailored to the organization's particular business and mission. Each should address the organization's business landscape associated with the state of technology, its organizational culture, its operating policies, the regulatory environment in which it operates, and the cloud security architecture towards which the organization is headed. For federal agencies, this is spelled out in CISA's Cloud Security Technical Reference Architecture.[11]

2.1 Technology

Technological considerations are critical. Legacy technology solutions have centered around adding layers to the perimeter, but this perimeter-based approach has been unable to contain the ever-increasing diversity and number of attacks on our IT systems. Computing units for application delivery have transitioned from concentrated big-iron servers to numerous virtualized servers

[11] Cybersecurity and Infrastructure Security Agency. (n.d.). *Cloud Security Technical Reference Architecture*. Retrieved September 29, 2021, from https://zerotrust.cyber.gov/cloud-security-technical-reference-architecture/

and services to highly granular containers distributed across a landscape of cloud properties. The atomization of function creates portability challenges for the application of ZT; however, given increased cloud adoption rates as part of digital transformation initiatives, ZT represents the next evolution and a modern cyber approach to prevention of and resiliency toward cyber-attacks. An organization's skill with key capabilities such as identity and credential access management (ICAM), software-defined networks (SDN), microsegmented environments, Identity-Aware Proxies (IAPs), and the ability to continuously monitor systems will drive the transition to ZT. Understanding the technology landscape in your architecture and the options available in the market ecosystem will influence the right solution for your environment.

2.2 Organizational Culture

An organization's culture is another strong influence for all stakeholders to consider. The COVID-19 pandemic has proven to be a catalyst pushing organizations into work-from-home programs and security teams to progress towards a ZT strategy. To adopt ZT, the organization must be willing to change and foster a "trust no one" approach through enterprise re-engineering. Proactive organizations embracing scalable cloud and hybrid models over legacy environments are at an advantage and will be able to more easily adopt the "ZT mindset." Understanding your culture and change management capability is essential.

2.3 Policy

Along with culture, the ability for an organization to update its policies is also critical. The modern IT organization is a sophisticated, complex, hybrid mix of on-premises and cloud-hosted architecture, which can make an organization's cybersecurity control policies challenging. The impact of changing policies permeates across an organization's entire infrastructure, applications, and data. The ability to identify and develop new ZT-based policies is an important factor and unique to each organization. Organizations may be challenged to identify, create, and formalize these policies, given the immaturity of ZTAs.

2.4 Regulatory Environment

A final influence highlighted in the adoption of ZT is the regulatory environment. The U.S. Government has two primary frameworks that drive cybersecurity compliance: the Risk Management Framework (RMF)[12] and Cybersecurity Framework (CSF), administered by NIST. They provide guidance on security assessment, implementation, authorization, and monitoring. Presidential Executive Order 13636 *Improving Critical Infrastructure Cybersecurity*,[13] issued on February 12, 2013, established a framework based on existing standards, guidelines, and practices for reducing cyber

[12] Securicon Team. (2019, October 8). *NIST 800–53 Rev. 5: What it Is, and Why You Should Care*. Securicon. https://www.securicon.com/nist-800-53-rev-5-what-it-is-and-why-you-should-care/

[13] Exec. Order No. 13636, 78 FR 11737 (February 12, 2013). https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

risks to critical infrastructure. This guideline reinforced the Cybersecurity Enhancement Act of 2014.[14] Although these compliance frameworks are flexible, they are not specifically or optimally honed to foster and promote effective ZTA implementations. Executive Order 14028 *Improving the Nation's Cybersecurity*,[15] issued on May 12, 2021, holds organizations accountable for managing cybersecurity risk and calls on the Executive Branch to support the cybersecurity efforts of critical infrastructure owners and operators, including its supply chain. These efforts are commendable in intent and build momentum for more policies; reference ZTAs such as the one the Department of Defense has built, coupled with the need for ZTA maturity assessments (ZTA-CMM) and ZTA roadmaps with a timeline to produce material improvements in security. These regulatory initiatives help to stimulate the changes necessary to thwart new cyber-attacks for greater cyber resilience. As new regulations are mandated, they will support industry providers and stakeholders such as hardware and software vendors, system integrators, service providers, IT organizations, and more introducing innovations into the solutions landscape.

[14] National Institute of Standards and Technology. (2021, July 14). *Cybersecurity Framework | Getting Started*. NIST. https://www.nist.gov/cyberframework/getting-started

[15] Exec. Order No. 14208, 86 FR 26633 (May 12, 2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

3 Zero Trust Solution Landscape

In order to advance your ZT maturity, it is essential to review and identify applicable technologies and solutions. For example, the traditional infrastructure for cloud computing has evolved and now includes modern components, such as containers and service mesh, that will require integration with ZT core components ("policy engine" [PE], an associated "policy administrator" [PA], and various "policy enforcement points" [PEP]).[16] These types of new strategies for managing ZTA will inevitably arise, and the following technological areas and related examples represent only a small sample of an evolving security landscape that offers modernized solutions towards a ZTA. The sample technology approaches and influences explored in this paper include a review of software-defined architecture components, service-mesh capabilities, edge computing trends, and policy as code possibilities.

3.1 Software-Defined Perimeter

A case can be made that a software-defined perimeter (SDP) and ZT principles evolved concurrently, responding to the same underlying pressures, realizations, and shifts in the security landscape. Furthermore, these concepts are well aligned, given that SDP components address many of the concerns that motivated ZT principles. Today, SDP is recognized by the industry as a distinct part of a software-defined architecture that can actualize ZT principles, and the NIST ZTA publication exhibits SDP as an approach to ZTA.[17]

Gartner Research characterizes SDP as a technology for providing "secure access to enterprise apps," highlighting device attestation and user authorization as an "intrinsic feature," along with "the ability to establish several encrypted tunnels to diverse destinations." [18] SDP provides access to application infrastructure only after device attestation and identity verification through real-time encrypted connections between requesting systems and application infrastructure. In 2019, Gartner continued to back SDP via their Zero Trust Network Access (ZTNA) model,[19] which creates an identity- and context-based logical-access boundary around an application or set of applications. The applications are hidden from discovery and access is restricted via a trusted broker to a set of named entities. This removes the application assets from public visibility and reduces the surface area for attack.[20] This evolution was also supported by the Cloud Security Alliance (CSA) in its 2020 report *Software-Defined Perimeter (SDP) and Zero Trust*[21] by recognizing a SDP as a "Network Layer Zero Trust."

[16] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August 11). *SP 800–207, Zero Trust Architecture*. NIST. https://csrc.nist.gov/publications/detail/sp/800-207/final

[17] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August 11). *SP 800–207, Zero Trust Architecture*. NIST. https://csrc.nist.gov/publications/detail/sp/800-207/final

[18] Gartner Research. (2018, November 9). *Fact or Fiction: Are Software-Defined Perimeters Really the Next-Generation VPNs?* https://www.gartner.com/document/3892882

[19] Riley, S., MacDonald, N., & Orans, L. (2019, April 29). *Market Guide for Zero Trust Network Access*. Gartner. https://www.gartner.com/en/documents/3912802/market-guide-for-zero-trust-network-access

[20] Riley, S., MacDonald, N., & Orans, L. (2019, April 29). *Market Guide for Zero Trust Network Access*. Gartner. https://www.gartner.com/en/documents/3912802/market-guide-for-zero-trust-network-access

[21] Cloud Security Alliance SPD and Zero Trust Working Group. (2020, May 27). *Software-Defined Perimeter (SDP) and Zero Trust*. Cloud Security Alliance. https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-and-zero-trust/

3.2 Network Segmentation

As discussed above, SDP provides an approach toward ZTA; however, it must also leverage segmentation (often referred to as microsegmentation in ZT literature) to reduce the attack surface via a default-deny model and obstruct lateral movement characteristic of data breaches. An SDP approach stems from the evolution in network segmentation capabilities that enforces authentication and authorization before allowing access. The addition of encryption to shared network links is a method of network segmentation by encryption key. Another approach, host-based segmentation, is the ability to control host firewalls to create authorized communications channels delivering dynamic policy and segmentation controls, at scale and across heterogeneous OS-compute platforms (on-premises, public and private cloud, and containers) and allows policies to follow the workload versus the use of encryption keys.

Using network segmentation for security requires the creation of security zones that are defined by a combination of the service type and its communication relationships, user identities, and data sensitivity for each zone.[22] Traditional network security zoning paradigms are challenged by resource overheads, the complexity of firewall rules management, and integration risks that can result in a limited set of fairly broad trust zones. This contradicts the "attack surface reduction/least privilege" philosophy of ZT. Further, organizations with modern application architectures that have workloads running on virtual machines, containers, stateless servers, and emerging technologies like containers, serverless, and managed cloud services may struggle to effectively segment with these traditional paradigms.

Software-defined networks (SDN), however, separate the network control plane that manages traffic from the forwarding plane. Network control is directly programmable via APIs, allowing for more dynamic adjustment of flows and segmentation controls to microsegment traffic. East-west segmentation via SDN allows for the creation of more granular security zones.

A microsegmentation solution should have integrations that provide comprehensive and unified visibility about the identity of a workload, device/endpoint, and user. Ideally, it can also enable automation and orchestration of segmentation for preventative and responsive security incident scenarios. As ZT capabilities mature, the ability to incorporate metadata labeling governance will support the automation and orchestration of segmentation controls. Examples include:

- Dynamic enforcement of allow-list in response to changes such as IP address, detection of new workload, user and device connections.
- Integration with DevSecOps CI/CD pipelines to provision segmentation "at birth" of new workloads and containers.
- Alerting and analytics to feed into dynamic policy management.
- Integration with threat detection, monitoring, and vulnerability scanning to automatically recalculate the applicable allow-list and orchestrate process-level segmentation.

As not all segmentation approaches are the same, organizations must choose the architecture and deployment model that best fits their cloud infrastructure.

[22] Riley, S., MacDonald, N., & Orans, L. (2019, April 29). *Market Guide for Zero Trust Network Access*. Gartner. https://www.gartner.com/en/documents/3912802/market-guide-for-zero-trust-network-access

Given the critical and pervasive role that cloud service providers (CSPs) play in providing IT organizations with secure, scalable, and agile computing and storage options, it is important to also note the ubiquitous adoption of SDPs and SDNs as an approach to ZTA by these providers. CSPs now leverage SDN as an integral component of their ZT approach to design, build, and operate global-scale IPv4 and IPv6 networks. This in turn supports improved security and expands the native services available to support ZT components for their vast customer base and partner ecosystems. Individual organizations will need to understand how they can best leverage any native components or additional third-party providers to design and implement their own ZTA as outlined by their roadmaps.

3.3 Service Mesh

Another important technology consideration in ZTAs is a container-based service mesh for achieving centralized policy management and orchestration. Containers have emerged as the preferred application construct in modern cloud computing environments, but while they create deployment efficiencies, they also have the potential to significantly increase the number of endpoints in IT architectures. If you are not using a service mesh, this poses challenges when attempting to broadly implement security policies across container environments.

Most new container environments are now being enabled by container platforms like Kubernetes, RedHat OpenShift, Docker Swarm, and Nomad, and cloud-based services like AWS Elastic Container Service (ECS).[23] Container platforms don't typically address intra-container communications security, and service mesh solutions have evolved to support the management, deployment, and real-time orchestration of communication security policy across container environments. Implementation of the sidecar container or process is the predominant approach. A sidecar is implemented to act as a Policy Enforcement Point (PEP), operating as a front-end security guard for container-based workloads. The PEPs in a Kubernetes cluster should be high-performance and secure proxies that can address policy enforcement as well as other security protections, such as those from web application firewalls (WAFs). A central orchestration service serves as a Policy Decision Point (PDP) for invoking cybersecurity policies, typically associated with access control and event monitoring. This intra-Kubernetes architecture should be well integrated with the control plane and the enterprise's ICAM services and support modern and legacy authentication standards.

An innovation in extending ZT to a containerized, microservices endpoint is the implementation of a service mesh such as ISTIO. ISTIO is an open-source service mesh that is transparent to an organization's existing Kubernetes-based containerized application offering.[24] It is well-tailored to support today's DevSecOps pipelines, as demonstrated by the Department of Defense Platform One.[25] The ISTIO solution can deliver a ZTA solution to an organization's container environment consistent with NIST SP 800-207 prescriptions.

[23] ClickIT. (2021, August 5). *The most popular Kubernetes alternatives and Competitors.* https://www.clickittech.com/devops/kubernetes-alternatives

[24] Istio. (n.d.). *Istio*. Retrieved September 29, 2021, from https://istio.io/

[25] Chaillan, N. (n.d.). *How did the Department of Defense move to Kubernetes and Istio?* NIST Computer Security Resource Center. Retrieved September 29, 2021, from https://csrc.nist.gov/CSRC/media/Presentations/dod-enterprise-devsecops-initiative/images-media/DoD%20Enterprise%20DevSecOps%20Initiative%20%20v2.5.pdf

3.4 Edge Computing

As modern application architectures based on Kubernetes become more prevalent and enterprises continue to turn to multiple cloud providers for elements of their IT infrastructure, there will arise a need to manage ZTA across multiple deployment locations (on-premises, in various clouds, and even at the network edge closest to the users). Computing at the "edge" is another evolving consideration that in the coming years will become increasingly vital for connected industries such as robotics, autonomous vehicles, augmented reality (AR), and more. This world of highly distributed applications will need all the components of the modern stack; however, computing at the edge securely and transparently to the user will introduce a need to enforce security, such as the ability to establish a ZTA across a "mesh" of distributed applications and their application origins (in the cloud or on-premises). This concept of distributed applications might be thought of as "Edge 2.0"[26] and will require a more mature ZTA design, given the increased complexity of extending traditional cloud infrastructure that processes local telemetry and/or requests for bi-directional data exchange.

3.5 Policy as Code

The last technological consideration of this paper is the upcoming significance of policy as code. The objective of policy as code is to unify policy enforcement across varying technologies (not limited purely to cloud-native). It does this through automating compliance and configuration enforcement within the CI/CD pipeline as well as ABAC and RBAC from a single declarative policy. This makes it ideal for hybrid and cloud environments that are trying to mature their ZTA.

Policy as code implements a declarative mechanism to enforce services compliance verification and access rules, enforcing desired state runtime controls through standardized evaluation of pre-deployment checks/tests (corporate and/or regulatory). This is an enabling technology approach to include for a ZTA because it is implemented as code using the same methods used for source control creating a documented audit trail. As such, rules defining operational access and interdependent services can be tagged or mapped against strict requirements of the application and service interfaces. It implements the framework to author policy instantiation across the cloud-native pipeline.

[26] Lin, G. (2021, February 8). *Edge 2.0 Manifesto: Redefining Edge Computing*. F5. https://www.f5.com/company/blog/edge-2-0-manifesto-redefining-edge-computing

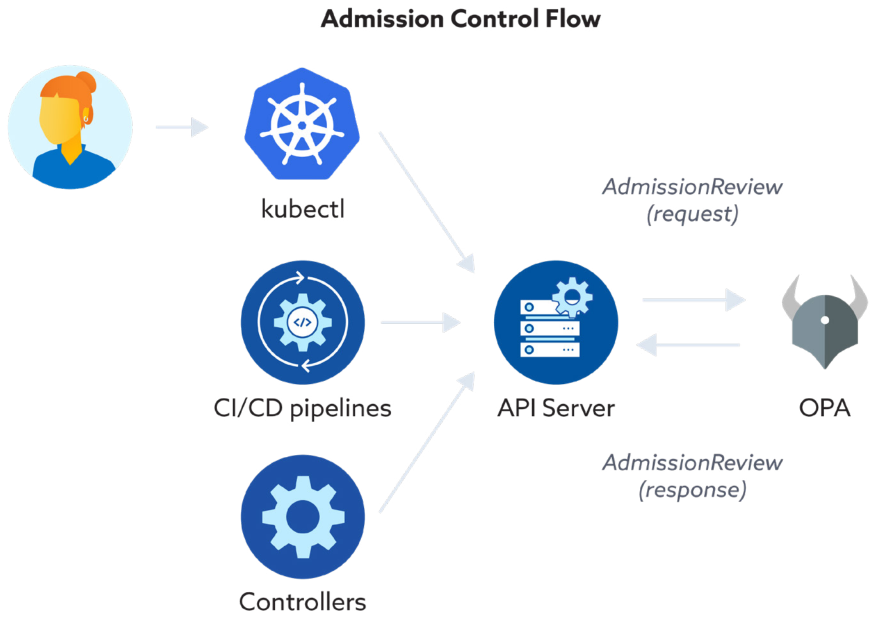


Figure 6. OPA Admission Controller, CNCF

Open Policy Agent (OPA) is a project initiated in 2018 and graduated in February 2021 through the Cloud Native Computing Foundation (CNCF)[27] to help define and apply policy as code. OPA is effectively an admission controller, a PEP, enforcing specific requirements and checks during the integration and deployment pipeline(s) through a declarative rules engine and automation

Figure 7. OPA-supported ZTA, OpenPolicyAgent.org

[27] Cloud Native Computing Foundation. (2021, February 4). *Cloud Native Computing Foundation Announces Open Policy Agent Graduation.* https://www.cncf.io/announcements/2021/02/04/cloud-native-computing-foundation-announces-open-policy-agent-graduation/

as illustrated in Figure 6. It is implemented as either a library or daemon with integrations for Kubernetes, API AuthZ, and Linux PAM environments. The application or service needing to enforce that policy consults OPA for a PEP decision at each API request.[28] It thereby enhances ZTA through enforcement of access and configuration policy consistency, as shown in Figure 7.[29]

3.6 Identity Aware Proxy

An example of policy as code is an Identity-Aware Proxy (IAP). Identity and context-awareness are the cornerstones of access in a ZTA. Identity and context, in combination with intent, are also the foundations for an IAP. An IAP requires a root of trusted identity to authenticate (verify) users and their devices as well as what they are authorized to access (authorization). This is identity-aware access. IAPs provide authenticated and authorized secure access to specific resources using a proxy layer. As such, IAPs allow the enterprise to retrofit ZT into their legacy network, placing an intelligent proxy in front of the applications which can enforce the enterprise security policy.

An IAP focuses on identity and access at the application layer and relies on access controls, not firewall rules. Configured policies reflect user and access intent, not ports and IP addresses. Further, IAP establishes a central authorization layer based on the principles of least privilege access and enforces access on a per-request basis, providing a ZT operational governance model. With IAP, any access request may be terminated, examined, or re-examined, modified, and authorized.

[28] Open Policy Agent. (n.d.). *OPA Ecosystem*. https://www.openpolicyagent.org/docs/latest/ecosystem/

[29] Open Policy Agent. (n.d.-b). *Open Policy Agent.* Retrieved September 29, 2021, from https://www.openpolicyagent.org/

4 Implications for Industry

The related implications of the solutions landscape are briefly examined in this section in terms of the key influences: technology, culture, policy, and regulatory initiatives. Although not exhaustive, these implications can help industry stakeholders identify the salient challenges and opportunities that require ongoing attention through industry collaboration in each area of consideration.

4.1 Technology

Given the rich and diverse technology solutions and capabilities that are emerging, the options for a robust ZTA are complex, plentiful, and promising. As IT organizations incorporate these evolved solutions as part of their ZTA, the security landscape will fundamentally reflect a different and improved approach to cybersecurity. As such, it also has the potential to bend the cost curve, meaning that, for once, we have a potential approach that substantially raises the cost to the attacker by having to achieve significantly more comprehensive and continuous verifications and that can lower the cost to the defender. There is an initial cost to implement a ZTA but, over time, other technologies will be less necessary and perhaps eliminated altogether as duplicative. Any discussion of economic or business impact will need to be debated by industry constituents as ZT standards mature. Such a sophisticated landscape also calls for ongoing guidance from the government on how the NIST Risk Management Framework (RMF) can help in developing and implementing a ZTA, as seen in the draft NIST publication *Planning for a Zero Trust Architecture: A Starting Guide for Administrators*.[30] Additional industry guidance is still needed to help IT and security experts understand how to assess, evaluate, and unify the myriad ZT approaches now available.

For example, with regards to SDPs and SDNs, the challenge of identifying the right elements of an SDP for each organizational environment is still outstanding. For example, is the boundary of the SDP enforced at the data, application, platform, or host level? In reality, a hybrid solution will likely evolve. This gap will require greater industry and government collaboration to provide guidance to organizational leaders on selecting the right elements for their environment. Nonetheless, ensuring greater maturity towards SDPs is vital to an organization's ZTA.

With regards to service mesh, future service delivery fabric(s) will become further distributed and more atomic. While both Kubernetes and service mesh architectures are generally agnostic to the components being implemented (e.g., containers, sidecar proxies), proper application of ZTA to containerized application environments will require some level of industry standardization on best practices, given the diversity of software and hardware components of today's hybrid environments. A bridge between components running on traditional hardware or virtual machine infrastructure (on-premises or in the cloud) and native container environments will be needed. The challenge for the industry will be to allow the core components of ZTA to be natively resident in the relatively small runtime container environments (e.g., disk and RAM requirements). This development may warrant consideration and guidance as part of the Trusted Internet Connection policy (TIC) evolutions from CISA and third-party cloud integrators.

[30] Rose, S. (2021, August 4). *Planning for a Zero Trust Architecture: A Starting Guide for Administrators.* NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.08042021-draft.pdf

4.2 Organizational Culture

As stated in the beginning, a propensity for change is critical to adopting ZT principles across the industry. To change business and security culture, a greater understanding of the various personas is needed. ZT may seem intimidating at first to an administrator or developer, and may be perceived as further limiting their access and ability to perform their jobs. Organizations will need to support and grow their talent and resources on understanding the benefits of adopting ZT principles and movement towards assessing their environments and implementing a defined roadmap. Once again, this will require executive support, a defined change management process, and capital and resource investments to design, evaluate, and implement a ZTA, which may be outside of current budget cycles.

4.3 Policy

Policy challenges will continue to persist in areas of interoperability and the management issues that arise in a dynamic cloud environment. Visibility, context, and control will form the modern organizational battlefield for the governance landscape. Thankfully, today’s ZT principles, frameworks, and architectures can help to guide organizational development in this challenge. First, an organization-wide policy will likely need to be revised or developed as new roles, processes, and technologies are adopted to achieve a ZTA. The fact that the cloud also supports multiple tenants across organizations presents a modern policy challenge. Simply put, some policies cannot be globally implemented. Further, as access policy and best practices evolve, policy logic will need to be managed externally to the application they secure but still support centralized management, which is necessary to achieve management economies. This concept is complicated in the multi-tenant/multi-system owner environment where the evolution of application development has strongholds in stove-pipe mentality that are slowly evolving with DevSecOps environments. Industry would benefit from the development of improved, more automated, and efficient policy management solutions as part of DevSecOps processes.

Policy as code continues to gain importance and the industry may be in a stronger position to develop and incorporate approaches for ZTA implementation throughout the software supply chain. DevSecOps and CI/CD pipelines are the new supply chain for applications and infrastructure and increasingly leverage container technology. ZTA cannot be ignored from implementation within and throughout CI/CD approaches in the software supply chain. Modern applications are sometimes partially composed of third-party vendor and open-source components that are often referred to as “dependencies.” As a result, the acquirer organization may have little visibility into the supply chains of its suppliers and organizations are impacted by more and different regulations with increased costs to audit new paradigms, such as ZTA. This can slow down adoption.

Even in edge computing, cybersecurity policy is implemented via the core OS and network and cloud services. There needs to be clear accountability on enforcing access, authorization, and accounting (AAA). Providers such as CDNs and CSPs strictly enforce AAA, required through regulations in an auditable and verifiable manner. This is at the core of “shared responsibility” and should remain as an accountability model for ZTAs in edge computing environments, with this perspective endorsed by industry as a best practice.

4.4 Regulatory Environment

It is not clear that security can be regulated by government authorities, but government policy can cultivate a focus on security and guide investment decision making. The recent Presidential Executive Order 14028, *Improving the Nation's Cybersecurity*,[31] is operating to do just that. But government policy must be established to foster and guide the development of a holistic view for cybersecurity solution implementation. No longer can application security be built into applications without consideration of available access, network, and data security capabilities. Interoperability and integrability must be hallmarks of a policy that fosters the adoption of ZT principles. The focus on data flows that address user interactions but do not address machine-to-machine communications will fall short in the long run. Policies that foster technology stove piping in the supply chain can only operate to create gaps in defenses.

[31] Exec. Order No. 14208, 86 FR 26633 (May 12, 2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

5 Recommendations

Through a broad exploration of ZT maturity and roadmap approaches, an evolving ZT landscape and the impact of technology, culture, policy, and regulatory factors, this paper provides a snapshot of the diversity, complexity, and infancy of ZT adoption. Although many topics have been presented, this evolution in security will be the topic of many ongoing industry discussions. For the purpose of this paper advocating the next actions to support industry-wide ZTA adoption, the following recommendations are provided:

The CISA ZTA capability maturity model (ZTA-CMM) assessment approach should be adopted, as prescribed in this paper. This maturity assessment should be conducted and the results should inform stakeholders on how they can develop a specific and priority-based ZTA roadmap to their targeted maturity level over a three-to-five-year timeline. This will in turn help to inform required resource allocations and technology evaluations or investments that need to be considered as part of a ZT roadmap and related enterprise planning cycles. Based on their target maturity and roadmap requirements, organizational leaders should adopt a "crawl-walk-run" approach in their roadmap requirements. Even after 10 years, innovation in ZT technologies, skill sets, and processes are all in their infancy.

Industry and government should continue to collaborate to provide organizations with ongoing guidance to evaluate ZT solutions that best fit their roadmap requirements. As already discussed in this paper, government and industry organizations are just beginning to explore a complex and evolving landscape to identify the solutions that can best address their ZT maturity goals. Many of these solutions will continue to evolve at the same time, making the evaluation process complicated.

As such, **leading organizations should continue to share their progress on solution evaluations through industry forums**. This will help in the identification of ZTA best practices that work in similar environments. Further, an ongoing collaboration of government and industry will help to accelerate ZTA adoption and move the industry towards standardization. This initiative is recently represented by the National Cybersecurity Center of Excellence (NCCOE) initiating a lab project to help evaluate a sample of technology options for ZT consideration.[32] The recent government reference paper to guide RMF requirements in ZT implementations previously referenced in this paper is another example of how the government is responding to industry. Another recommended industry initiative is a national CSA ZT Working Group to help capture and coalesce industry stakeholder voices across a rich ecosystem of component manufacturers (hardware/software), system integrators, service providers, and more.

[32] National Cybersecurity Center of Excellence. (n.d.). *Zero Trust Architecture*. NIST NCCoE. Retrieved September 29, 2021, from https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

Lastly, it is recommended that **the vendor ecosystem should reevaluate its capability to address the range of ZTA requirements, from policy automation to real technology capabilities that promote interoperability, control, and context**. The more transparent solutions that can quickly identify and share their unique role in the ZT landscape, the faster IT organizations will be able to attract early adopters and continue to mature their capabilities for more secure national and global infrastructure. Solution providers should be proactive and seek client-partner relationships to promote a comprehensive and easy evaluation cycle, supporting new efficiencies and helping to identify solutions that can be sunset in today's modern era at low cost to the user.

6 Additional Reading

Defines SDN: Aliyu, A. L., Aneiba, A., Patwary, M., & Bull, P. (2020). A trust management framework for Software Defined Network (SDN) controller and network applications. *Computer Networks, 181.* https://doi.org/10.1016/j.comnet.2020.107421

Provides Cloud and Trust Taxonomy based upon IaaS: Ibrahim, F. A. M., & Hemayed, E. E. (2019). Trusted Cloud Computing Architectures for infrastructure as a service: Survey and systematic literature review. *Computers & Security, 82,* 196–226. https://doi.org/10.1016/j.cose.2018.12.014

Provides a Cloud Security Taxonomy: Mthunzi, S. N., Benkhelifa, E., Bosakowski, T., Guegan, C. G., & Barhamgi, M. (2020). Cloud computing security taxonomy: From an atomistic to a holistic view. *Future Generation Computer Systems, 107,* 620–644. https://doi.org/10.1016/j.future.2019.11.013

Ruan, Y., & Durresi, A. (2019). A trust management framework for clouds. *Computer Communications, 144,* 124–131. https://doi.org/10.1016/j.comcom.2019.05.018

Scott, B. (2018). How a zero trust approach can help to secure your AWS environment. *Network Security, 2018(3)*, 5–8. https://doi.org/10.1016/s1353-4858(18)30023-0

National Security Agency. (2021, February). *Embracing a Zero Trust Security Model.* U.S. Department of Defense. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

FedRAMP. (2017, November 15). *FedRAMP Security Assessment Framework*. https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf

National Institute of Standards and Technology. (2018, December). *NIST Special Publication 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations*. NIST. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

7 References

American Council for Technology-Industry Advisory Council. (2019, April 18). *Zero Trust Cybersecurity Current Trends*. https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf

Chaillan, N. (n.d.). *How did the Department of Defense move to Kubernetes and Istio?* NIST Computer Security Resource Center. Retrieved September 29, 2021, from https://csrc.nist.gov/CSRC/media/Presentations/dod-enterprise-devsecops-initiative/images-media/DoD%20Enterprise%20DevSecOps%20Initiative%20%20v2.5.pdf

ClickIT. (2021, August 5). *The most popular Kubernetes alternatives and Competitors*. https://www.clickittech.com/devops/kubernetes-alternatives/

Cloud Native Computing Foundation. (2021, February 4). *Cloud Native Computing Foundation Announces Open Policy Agent Graduation*. https://www.cncf.io/announcements/2021/02/04/cloud-native-computing-foundation-announces-open-policy-agent-graduation/

Cloud Security Alliance SPD and Zero Trust Working Group. (2020, May 27). *Software-Defined Perimeter (SDP) and Zero Trust*. Cloud Security Alliance. https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-and-zero-trust/

CMMC Information Institute. (2021, August 21). DoD/NIST SP 800–171 Basic Self Assessment Scoring Template. https://cmmcinfo.org/cmmc-info-tools/dod-nist-sp-800-171-basic-self-assessment-scoring-template/

Cybersecurity and Infrastructure Security Agency. (n.d.). *Cloud Security Technical Reference Architecture*. Retrieved September 29, 2021, from https://zerotrust.cyber.gov/cloud-security-technical-reference-architecture/

Cybersecurity and Infrastructure Security Agency, Cybersecurity Division. (2021, June). *Zero Trust Maturity Model - Pre-decisional Draft, Version 1.0*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

Exec. Order No. 13636, 78 FR 11737 (February 12, 2013). https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Exec. Order No. 14208, 86 FR 26633 (May 12, 2021). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Forrester. (n.d.). *The Zero Trust Security Playbook For 2021*. Retrieved September 29, 2021, from https://www.forrester.com/playbook/The+Zero+Trust+Security+Playbook+For+2020/-/E-PLA300

Gartner Research. (2018, November 9). *Fact or Fiction: Are Software-Defined Perimeters Really the Next-Generation VPNs?* https://www.gartner.com/document/3892882

Istio. (n.d.). *Istio*. Retrieved September 29, 2021, from https://istio.io/

Kindervag, J. (2010, September 17). *No More Chewy Centers: Introducing the Zero Trust Model of Information Security*. Palo Alto Networks. https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

Lin, G. (2021, February 8). *Edge 2.0 Manifesto: Redefining Edge Computing*. F5. https://www.f5.com/company/blog/edge-2-0-manifesto-redefining-edge-computing

Microsoft. (n.d.). *Zero Trust Model - Modern Security Architecture*. Retrieved September 29, 2021, from https://www.microsoft.com/en-us/security/business/zero-trust

National Cybersecurity Center of Excellence. (n.d.). *Zero Trust Architecture*. NIST NCCoE. Retrieved September 29, 2021, from https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

National Institute of Standards and Technology. (2021, July 14). *Cybersecurity Framework | Getting Started*. NIST. https://www.nist.gov/cyberframework/getting-started

Open Policy Agent. (n.d.). *OPA Ecosystem*. https://www.openpolicyagent.org/docs/latest/ecosystem/

Open Policy Agent. (n.d.-b). *Open Policy Agent*. Retrieved September 29, 2021, from https://www.openpolicyagent.org/

Riley, S., MacDonald, N., & Orans, L. (2019, April 29). *Market Guide for Zero Trust Network Access*. Gartner. https://www.gartner.com/en/documents/3912802/market-guide-for-zero-trust-network-access

Rose, S. (2021, August 4). *Planning for a Zero Trust Architecture: A Starting Guide for Administrators*. NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.08042021-draft.pdf

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August 11). *SP 800–207, Zero Trust Architecture*. NIST. https://csrc.nist.gov/publications/detail/sp/800-207/final

Securicon Team. (2019, October 8). *NIST 800–53 Rev. 5: What it Is, and Why You Should Care*. Securicon. https://www.securicon.com/nist-800-53-rev-5-what-it-is-and-why-you-should-care/

U.S. Office of Management and Budget. (n.d.). *Federal Zero Trust Strategy*. Cybersecurity & Infrastructure Security Agency. Retrieved September 29, 2021, from https://zerotrust.cyber.gov/federal-zero-trust-strategy/