National Security Agency | Cybersecurity Information

Advancing Zero Trust Maturity Throughout the Application and Workload Pillar

Executive summary

In the current digital landscape where malware and emerging online threats continue to evolve and become more sophisticated, it is imperative that organizations prioritize cybersecurity as essential to their operations. Information Technology (IT) professionals are keenly aware of the security challenges facing applications, but workloads are every bit as important to consider in this domain.

Workloads represent computational tasks, which encompass multiple programs or applications performing those tasks by utilizing computing, data, networking, and storage resources. Workloads evolve over their lifecycle through mission development, test, and production scenarios. “A workload is an expression of an ongoing effort of an application AND what is being requested of it … Applications tend to shape the characteristics of the workload itself by how it processes the data, or the software limits inherent to the solution.” [1] Workloads can be comprised of services across multiple clouds, with application programming interfaces (APIs) connecting to third parties and sensitive databases that require different levels of access. To navigate the complexities of managing workloads across computing environments and workflows, organizations are turning to advanced tools such as backend APIs, workload automation software, artificial intelligence (AI) predictive analytics, and cloud management platforms. [2]

These tools enable organizations to achieve their mission of interconnectedness, scalability, and usability by interacting with and exchanging data. This exchange of data creates opportunities for malicious actors to target business applications and workloads, as well as the methods used to safeguard them, leading to security challenges.

This cybersecurity information sheet (CSI) provides recommendations for achieving progressive levels of application and workload pillar capabilities and further discusses how these capabilities integrate into a comprehensive Zero Trust (ZT) framework. [3] National Security System (NSS), Department of Defense (DoD), and Defense Industrial Base (DIB) owners should use this and other guidance to develop concrete steps for maturing their application and workload security.

Introduction

Traditionally, access to applications was granted at the local level and was static, meaning that once authorization was granted it remained in place until it was revoked. A ZT model, however, shifts this paradigm to a ‘never trust, always verify’ model. This ZT model supports modern environments, such as hybrid clouds, edge locations, and container deployments; and to better secure networks from current threats, organizations must channel efforts into a more integrated security architecture focused on protecting data, applications, assets, and services (DAAS). The DoD ZT Security Model is best illustrated as seven pillars comprising the complete cybersecurity posture. [4]

Adopting a ZT framework bolsters the protection of critical applications and workloads with a decisive shift from a network-centric to a data-centric security model (DSM) and granular implementation of attribute-based access control (ABAC) for every data access. A modernized ZT framework integrates visibility from multiple vantage points, makes risk-aware access decisions, and automates detection and response. The application and workload pillar disrupts the efforts of malicious actors by bringing granular access control and visibility to applications and workloads in the environment.

By implementing this ZT security model, applications are hidden from unauthorized users and there is no ability to scan for resources beyond the requested application. Organizations that have robust identity management for authorized users and have integrated continuous automated monitoring into their security strategy will have full visibility to trace every transaction and pinpoint exactly what each workload is doing at any given moment. The workloads enforce granular, consistent access control to applications across disparate data center and cloud environments. Implementing such a framework places cybersecurity practitioners in a better position to secure sensitive DAAS. [3]

The spectrum of applications and workloads includes individual tasks on end-user systems, services executing on on-premises servers, and applications or services running in cloud environments. ZT workloads span the complete application stack from the application layer to the hypervisor. Securing and properly managing the application layer as well as compute containers and virtual machines is central to ZT adoption. [4]

This CSI details progressively maturing capabilities in the application and workload pillar. It includes recommendations and examples for achieving increasing maturity levels, from initial preparation, through the basic and intermediate phases, and finally to the advanced ZT level for making well-informed, risk-aware, fine-grained access decisions.

Audience

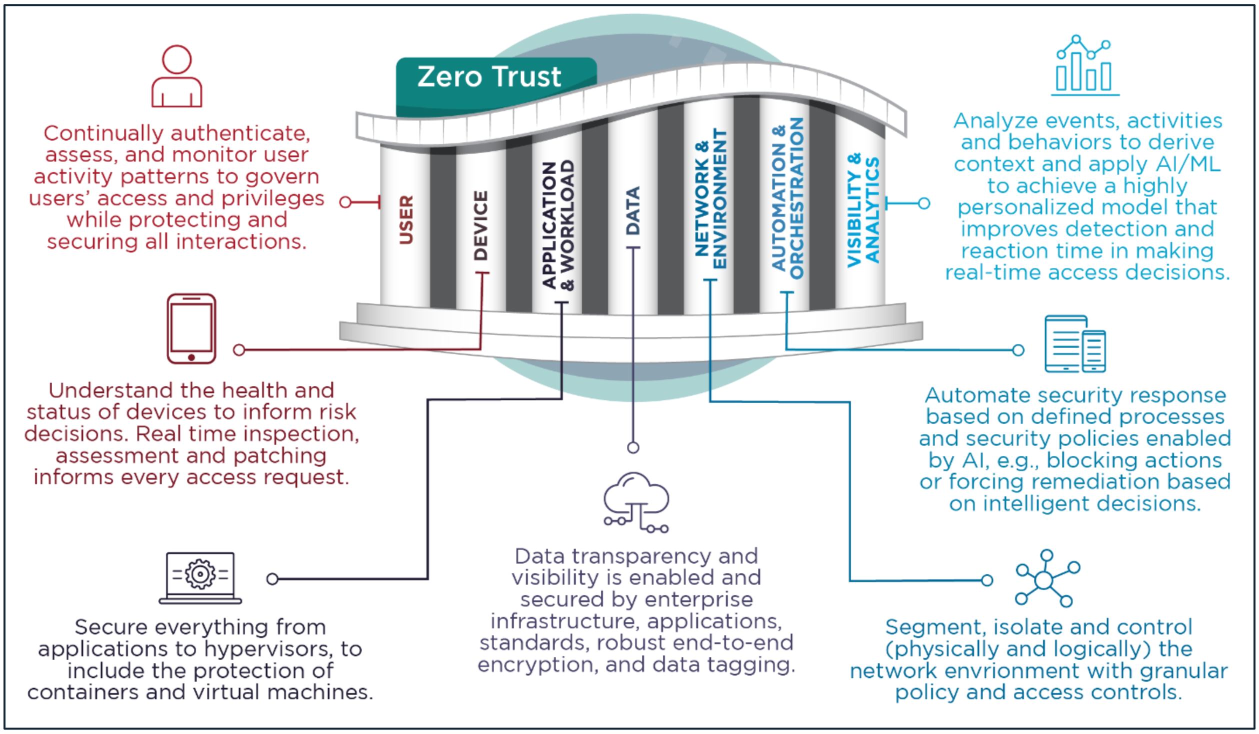
This CSI provides guidance primarily intended for NSS, DoD, and the DIB, but may be useful for owners and operators of other systems that might be targeted by sophisticated malicious actors. Guidance for other system owners and operators is also available via the National Institute of Standards and Technology (NIST) [5] and the Cybersecurity and Infrastructure Security Agency (CISA). [6] This guidance is compatible with the DoD's Cybersecurity Reference Architecture (CS RA) Version 5.0, [7] the DoD ZT Reference Architecture (ZT RA) Version 2.0, [4] and the DoD ZT Strategy. [8]

Background

The President's Executive Order on Improving the Nation's Cybersecurity (EO 14028) [9] and National Security Memorandum 8 (NSM-8) [10] direct the Federal Civilian Executive Branch (FCEB) agencies and NSS owners and operators to develop and implement plans to adopt a ZT cybersecurity framework. ZT implementation efforts are intended to continually mature cybersecurity protections, responses, and operations over time. Progression of capabilities in each of the seven pillars should be seen as a cycle of continuous improvement based on evaluation and monitoring of threats. [3]

This CSI offers guidance in accordance with the DoD ZT RA maturity scale of preparation, baseline, intermediate, and advanced. It also complements the DoD ZT Portfolio Management Office (PfMO) guidance of "target" and “advanced” levels. [8]

Figure 1 depicts the ZT pillars, including the application and workload pillar. The capabilities and milestones for this component of the ZT maturity model are described in detail throughout this document. Even though they are depicted separately, it is important to note that the pillars are not independent; many capabilities in each pillar depend on or align with capabilities in other pillars.



Continually authenticate, assess, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.

Understand the health and status of devices to inform risk decisions. Real time inspection, assessment and patching informs every access request.

Secure everything from applications to hypervisors, to include the protection of containers and virtual machines.

Data transparency and visibility is enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.

Analyze events, activities and behaviors to derive context and apply AI/ML to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

Automate security response based on defined processes and security policies enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions.

Segment, isolate and control (physically and logically) the network envrionment with granular policy and access controls.

Figure 1: The seven Zero Trust pillars

Application and workload pillar

Application security is the ability to secure an application by preventing exceptions to the application or the underlying information system's security policies. The application and workload pillar focuses on securing access at the application layer by integrating capabilities from the user, device, and network and environment pillars to prevent data collection, unauthorized access, or tampering with critical processes or services. In advanced ZT infrastructures, users strongly authenticate into applications, as well as underlying networks. [11] Applications are further secured with a reduced attack surface, by following principle 1.1 from the DoD CS RA that states least privilege should be incorporated by configuring systems to provide only essential capabilities. [7]

Applications and workloads are mutually dependent. Applications include any computer programs and services that execute in on-premises and cloud environments. While applications are the individual tools that serve business needs, workloads can be standalone solutions or tightly coupled groups of processing components performing mission functions. Workload implementations should dynamically segregate processing components and compute containers by filtering and applying access rules between components to increase the logical separation between critical resources and threat actors. Granular access controls and integrated threat protections can offer enhanced situational awareness and mitigate application-specific threats. [6] The application and workload pillar depends on the following key capabilities:

- Application inventory
- Secure software development and integration
- Software risk management
- Resource authorization and integration
- Continuous monitoring and ongoing authorizations

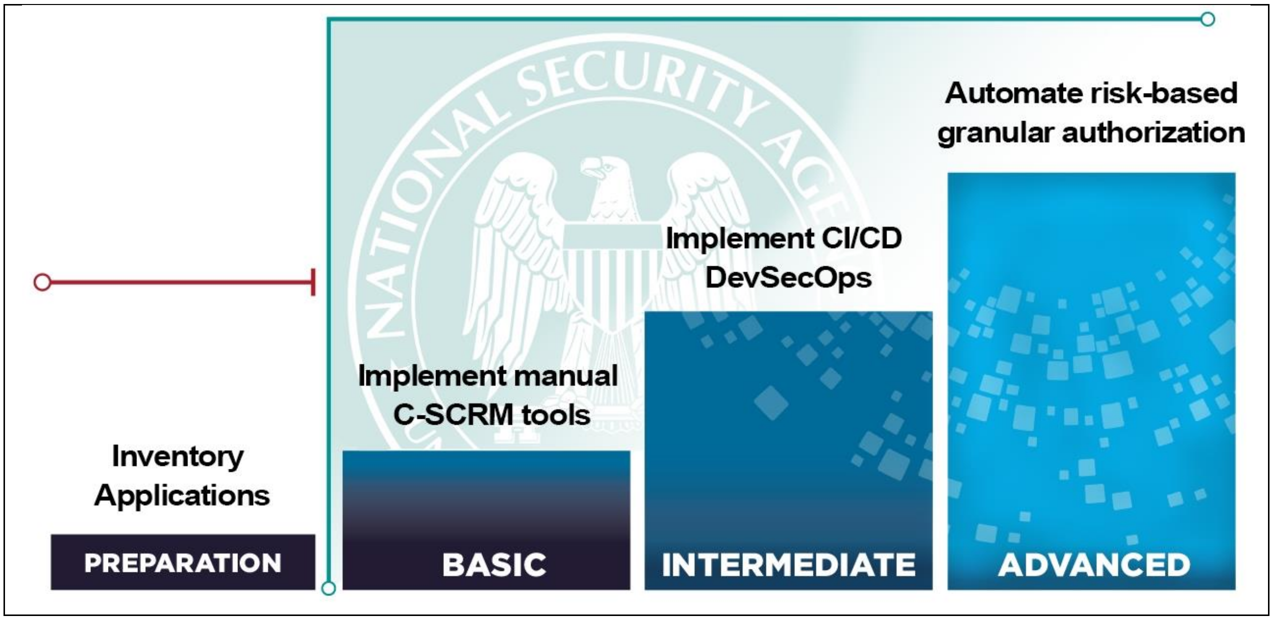

Inventory Applications
PREPARATION
Implement manual C-SCRM tools
BASIC
Implement CI/CD DevSecOps
INTERMEDIATE
Automate risk-based granular authorization
ADVANCED

Figure 2: Application and workload pillar maturity

Application inventory

Conducting an inventory of applications and workloads is a critical first step to implementing ZT. These resources must be identified and categorized to prioritize cybersecurity protection requirements for critical assets, especially of application updates.

An inventory of organizational application assets is a crucial yet effective ZT approach to increase an organization’s cybersecurity posture. Organizations must identify and categorize applications needed for critical workflows. Just as with user access, application identities should facilitate authentication to other necessary services based on the principle of least privilege (PoLP). Local directories and identity and access management (IAM) solutions can be used for administering application identities and facilitating access based on requisite conditions. Major cloud services offer central controllers to handle these tasks as well.

Additionally, utilizing this approach to inventory applications allows workflows to be prioritized and expedites the elimination of unapproved and/or unused applications, thereby reducing the attack surface and removing potential gaps and vulnerabilities in security.

Table 1: Application inventory maturity

Preparation	Basic	Intermediate	Advanced
Establishment of a scalable, well-functioning asset (or configuration) management program that collects the application inventory. It preferably implements application allow/deny listing to enforce policies on use of authorized applications.	Organizations conduct a thorough assessment of the current IT environment and user's needs. They create an inventory of existing applications and begin mapping workflows. Mapping is primarily manual at this level. Organizations begin including contract language requiring the delivery of Software Bills of Material (SBOMs) with all software deliverables. Organizations have established mechanisms to receive SBOMs and implement configuration management.	Organizations have a complete list of applications and identified critical workflows, with some automation implemented to maintain the list. The application inventory includes corresponding SBOMs in approved formats that detail software components. At a minimum, all direct component dependencies are identified and documented with the National Telecommunications and Information Administration (NTIA)-specified minimum fields. Transitive dependencies (component dependency on other components) are identified, even if the corresponding	Organizations have a complete inventory of applications and workloads. Only approved and required applications exist, all with proper, up to date SBOM documentation. SBOMs include component details for all direct dependencies. Transitive component dependencies are also documented. Open source components or components lacking NTIA-specified minimum field documentation are appropriately flagged as such. Additionally, procedures and automated tools help track and verify remediation of identified vulnerabilities on

Preparation	Basic	Intermediate	Advanced
	Procedures are established to address and track remediation of identified vulnerabilities.	component details aren't available. Organizations begin planning the removal/isolation of unused applications.	enterprise software assets.

Secure software development and integration

Most organizations rely on software and code from sources that could contain vulnerabilities or malicious injected functionality. Having secure software that can be relied on to perform its intended functions and not be exploited to perform malicious operations is just as important, if not more important, as securing the provided software. The ZT model recommends adopting the DevSecOps framework [12] and utilizing the continuous integration/continuous delivery (CI/CD) approach for organizations that develop applications to ensure secure development and deployment. [13] Developed source code and common libraries should be vetted through DevSecOps development practices to secure applications from inception. [14]

This ZT approach entails incorporating security controls through every phase of the development and deployment process. CISA outlines the concept of "Secure by Design" software development in which security considerations are made during the initial software design phase. This ensures the number of exploitable flaws are reduced before that software hits the market, and the total number of flaws are significantly fewer over the entire lifecycle of the software. [15]

Consequently, organizations should address the security of all APIs and implement network micro segmentation to isolate applications and workloads. Micro segmentation can help alleviate security challenges by creating separate logical network segments dedicated to the application's traffic.

Another security measure that is essential to the security of all applications is using strong encryption algorithms to ensure data the application relies on is protected both at rest and in transit.

Relatedly, digital signatures are essential to maintaining authenticity and integrity of applications. Digital signatures can help track software origins and maintain a reliable chain of custody. They are cryptographic hashes of the application's code that are encrypted with developer keys and decrypted by the user to compare with the hash value of the version being implemented to determine the software's integrity and origin. In addition, application containers should be digitally signed and verified before use to validate their integrity as well. Depending on the pipeline and capabilities, configurations may also be digitally signed to further build trust that the configuration of the application is as intended.

When working with containerized workloads, ensure their security by regularly scanning container images for vulnerabilities, limiting container privileges, protecting container secrets, and implementing runtime security controls.

Table 2: Secure software development and integration maturity

Preparation	Basic	Intermediate	Advanced
None at this level.	Organizations that develop software and application security processes begin to implement DevSecOps, to include ZT principles and best practices into all development efforts. Applications are digitally signed. Software is delivered with accompanying SBOM identifying, at a minimum, the software's direct dependency components. Continuous monitoring is in place for the components to identify factors (such as discovered vulnerabilities or emergent risky	Organizations that develop software implement CI/CD practices. DevSecOps integrates static and dynamic application security testing into software delivery workflows in accordance with the organization's requirements. DevSecOps also includes software component analysis that extracts NTIA specified minimum SBOM field information for each component in the build process. SBOMs are maintained and shared appropriately across the development and integration process. Components include hashes using a commonly recognized hash algorithm (such as SHA256) that can be	Organizations that develop software use process isolation and microsegmentation. DevSecOps and ZT security concepts, processes, and capabilities are fully adopted and integrated with CI/CD best practices throughout the entire development process. Automated software analysis includes identification and documentation of all software dependencies, including components or services loaded at run-time (e.g., remote procedure calls, calls to OS hosted libraries, data feeds for AI applications, microservices,

Preparation	Basic	Intermediate	Advanced
	organizational affiliations) that increase software risk profiles.	predictably compared to a source of truth.	and other third-party services).

Software risk management

Vendors offer solutions with attractive benefits to meet the needs of public and private sector customers. However, along with these attractive benefits comes increased potential for direct or indirect cybersecurity risks traveling throughout the supply chain. All software solutions carry some inherent risks. Prior to implementation, organizations should research planned IT solutions to determine suitability and whether their security features and capabilities meet quality and resiliency expectations.

"Deployed software is typically a commercial off-the-shelf (COTS) product, which includes smaller COTS or open source software components developed or sourced at multiple tiers. Updates to software deployed across enterprises often fail to update the smaller COTS components with known vulnerabilities." [16] This creates multiple risk factors for the software, especially when its underlying dependencies are themselves vulnerable. Organizations should determine if the use of such software is worth the risk, if they are capable of managing that risk, and how best to manage that risk.

Managing software risk involves calculating risk against need and ensuring that components of the supply chain are secure, vulnerabilities are reduced, and the organization is aware of residual risks. Organizations must ensure that all needed resources are available and allocated to allow continual validation of these risks and their mitigations. Those resources must also comply with modern authorization policies that limit access based on the principle of least access and implement ABAC for granular access decisions, or else be placed behind application gateways or proxies. Proxies or application firewalls may also be used to mitigate other application risks, such as application vulnerabilities and exploitation attempts. Regular security assessments, including penetration testing and vulnerability scanning, should be conducted to identify and remediate security weaknesses and risks proactively.

NIST's Cybersecurity Supply Chain Risk Management (C-SCRM) publication is designed to provide guidance to organizations on how to identify, assess, select, and implement risk management processes and mitigating controls. C-SCRM is a systematic process developed for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. [16]

NIST further cites specific guidance on integrating C-SCRM into enterprise risk management processes such as: a general prioritization model of C-SCRM practices, tailoring implementation to an enterprise's specific needs, knowing and managing critical products and services, working closely with critical suppliers, and frequently assessing and monitoring supply chain relationships. [16]

Table 3: Software risk management maturity

Preparation	Basic	Intermediate	Advanced
As part of developing an active C-SCRM program, prioritization of products and services is defined along with policies for accepting and mitigating application risks. Organizations inventory and assess their supply chains to ensure all entities are known and validated. A C-SCRM monitoring and assessment plan is established.	Organizations employ tools or a service to research n-tier relationships and risk attributes of suppliers before they purchase items from those suppliers that can potentially impact the application risk profile.	To the fullest extent possible, organizations implement a validation process of all software delivered through the supply chain to the component level. Organizations augment their software C-SCRM tools with threat intelligence to flag any software identified as having a supply chain compromise or increased risk profile for additional testing and validation.	Organizations implement an automated continuous monitoring system with integrated threat intelligence and testing to isolate and mitigate any software identified as having a supply chain compromise.

Resource authorization and integration

Resource authorization enables integration between assets in a lower risk manner by authenticating and limiting all accesses and removing access when no longer needed. Organizations should ensure resource authorization can be done programmatically through a standardized, secure API. Applications (often referred to as "legacy applications") that cannot adhere to modern, dynamic resource authorization policies that limit their access based on PoLP, ABAC, and changing environment conditions should be placed behind application gateways or proxies and planned for replacement by ones that can.

Applications and workloads may need their own accounts or authentication credentials, such as certificates or API keys, to authenticate to resources and other applications. The access granted by these credentials should follow PoLP and limit access to only what is needed for the intended application functionality and integration.

Table 4: Resource authorization and integration maturity

Preparation	Basic	Intermediate	Advanced
None at this level.	Organizations manually implement static rules and configurations to control access to applications and resources. Organizations begin to profile access behaviors to implement access control based on contextual information.	Organizations automate application access decisions based on contextual information and enforce time-based access. The decision criteria include a comparative analysis of the criticality of the mission vs. a risk score of the application. Application risk scores include a component for C-SCRM risk.	Organizations implement continuous application access authorizations using real-time automated risk analysis and behavioral analytics. Automated mechanisms monitor/mitigate the introduction of unauthorized applications or anomalous workflows.

Continuous monitoring and ongoing authorizations

Continuous monitoring and ongoing authorization are based on the idea that nothing is constant, there are continuous changes, and those changes can introduce vulnerabilities. Automated tools and processes should continuously monitor the health, status, and operability of deployed applications and workloads. Dashboards and alerts should be used to observe the status and changes to the workload, and alert appropriate personnel of significant changes. Implementing these processes will greatly enhance the overall security and incident response times for the organization.

Table 5: Continuous monitoring and ongoing authorizations maturity

Preparation	Basic	Intermediate	Advanced
None at this level.	Organizations collect log data related to applications and device health, status, and operability to populate a dashboard. Authorization decisions are made manually.	Organizations expand automated capabilities of the dashboard to revoke/limit access to applications automatically. Limited critical user access is managed manually. Access decision criteria compare and analyze the criticality of the mission vs risk score of the application. Application risk scores include a component for C-SCRM risk.	Organizations implement fully automated continuous authorizations and monitoring for users and applications based on anomalous behavior detection and threat intel. Automated mechanisms continuously check for known vulnerabilities in software elements. The automated continuous monitoring system integrates real-time assessment of application risks as part of the application access process.

Summary of guidance

The information presented here is not a standardized solution that fits all organizations, but rather suggestions and considerations for implementing ZT concepts related to applications and workloads. Discovering and defining the organization’s mission and identifying the supporting assets that need to be secured will help build a clearer picture of the as-is architecture which can be compared against the recommendations in this pillar along with the other ZT pillar CSIs.

Each organization will need to evaluate their individual requirements to determine a suitable solution. Ultimately, the goal is to develop a ZT roadmap that aligns with the organization’s ZT goals. The following guidance are the key ideas for implementing the ZT application and workload pillar to secure and protect against adversarial abuse of applications and workloads:

- Identify applications/workloads within or connecting to the environment.
- Ensure applications implement strong continuous authentication and granular access decisions, preferably leveraging available contextual information, as a precondition for the use of the applications and workloads.

- Follow PoLP, ensuring users and applications receive only the minimum level of access required to perform their jobs.
- Implement micro segmentation to limit lateral movement from applications and workloads.
- Employ continuous monitoring and logging to track anomalous and suspicious behavior.
- Utilize strong encryption algorithms to encrypt data in transit and at rest to ensure data integrity and confidentiality.
- Implement regular patch management for all applications and workloads.
- Ensure container security for containerized workloads by scanning container images for vulnerabilities, limiting container privileges, protecting container secrets, and implementing runtime security controls.
- Secure APIs by implementing authentication, authorization, and encryption mechanisms.
- Conduct regular security assessments, including penetration testing and vulnerability scanning, to identify and remediate security weaknesses proactively.
- Ensure application development and implementation compliance with relevant mandatory regulations and standards.
- Exercise due diligence and research to determine if IT solutions are fit for purpose, to include security features and capabilities meeting quality and resiliency expectations.

Further guidance

NSA is assisting NSS community members that are piloting ZT capabilities, coordinating ZT activities with NIST, CISA, and DoD, and developing additional ZT guidance to support system developers through the challenges of integrating ZT within NSS, DoD, and DIB environments. Upcoming additional guidance will help organize, guide, and simplify incorporating ZT principles and designs into enterprise networks.

Works cited

[1] P. Koehler. What is a Workload? 2021. https://core.vmware.com/blog/what-workload

[2] IBM. What is a workload? 2024. https://www.ibm.com/topics/workload

[3] National Security Agency. Embracing a Zero Trust Security Model. 2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

[4] Department of Defense. Department of Defense (DoD) Zero Trust Reference Architecture v. 2.0. 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[5] National Institute of Standards and Technology. NIST Special Publication 800-207: Zero Trust Architecture. 2020. https://csrc.nist.gov/publications/detail/sp/800-207/final

[6] Cybersecurity and Infrastructure Security Agency. Zero Trust Maturity Model. 2023. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

[7] Department of Defense. Cybersecurity Reference Architecture. 2023. https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf

[8] Department of Defense. DoD Zero Trust Strategy. 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[9] The White House. Executive Order on Improving the Nation’s Cybersecurity. 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[10] The White House. National Security Memorandum 8. 2022. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

[11] The White House. Federal Zero Trust Strategy Memorandum 22-09. 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[12] National Institute of Standards and Technology. Computer Security Resource Center (CSRC) DevSecOps. 2023. https://csrc.nist.gov/projects/devsecops

[13] National Security Agency et al. Defending Continuous Integration/Continuous Delivery (CI/CD) Environments. 2023. https://media.defense.gov/2023/Jun/28/2003249466/-1/-1/0/CSI_DEFENDING_CI_CD_ENVIRONMENTS.PDF

[14] National Institute of Standards and Technology. Secure Software Development Framework (SSDF). 2024. https://csrc.nist.gov/projects/ssdf

[15] Cybersecurity and Infrastructure Security Agency. Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software. 2023. https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf

[16] National Institute of Standards and Technology. Special Publication 800-161r1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of the authoring organization's cybersecurity mission, including their responsibilities to identify and disseminate threats, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
General Cybersecurity Inquiries or Customer Requests: Cybersecurity_Requests@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov