WaTech
Washington Technology Solutions

Zero Trust Security

WHITE PAPER

This white paper explores Zero Trust security, detailing how continuous verification of user identities and device integrity enhances protection against evolving cyber threats.

March 2025
Mikel B. Costello

Contributors

Zack Ashliman, Solution Architect

Ted Carroll, Telephony Cloud Solution Architect

Gerges Hana, Systems Engineer

Andrew Johnson, Enterprise Architect

Daniel Langley, Security Operations Center Manager (Acting)

Reanne Metzger, Systems Engineer

Doug Miller, Capacity Management Analyst

Greg Moore, Systems Engineer

Richard O’Keeffe, Capacity Management Analyst

Chris Patchett, Solution Architect

Cesar Rivera, Assistant Director, Network Services Division

Jerry Shaver, Systems Engineer

Larry Thornton, Systems Engineering Supervisor

Table of Contents

Executive Summary

WaTech is statutorily obligated to ensure the Confidentiality, Integrity, and Availability (CIA) of information transacted, stored, or processed within Washington State's IT systems and infrastructure. WaTech must also develop a centralized cybersecurity protocol to protect and manage state IT assets, detect and respond to security incidents in alignment with established standards and policies, and ensure business continuity for state operations during such incidents.[1]

As the Washington State government continues to support a remote work model, WaTech must evolve its security framework to support a telecommuting workforce. Currently, WaTech's SSL VPN service does not meet customer requirements, as it relies on routing remote connections through on-premises data centers before accessing external applications, causing inefficiencies and sub-optimal traffic flows. In addition, existing security protocols fall short in adequately protecting state-owned endpoints such as laptops, desktops, and mobile devices from data breaches and exploitation.

The volume of cyber-attacks targeting WaTech continues to rise exponentially, and existing defenses are no longer sufficient. To address the growing cybersecurity threat, WaTech must modernize its enterprise architecture, security technology, and adopt advanced security best practices. Past incidents have demonstrated how malware originating from one agency can spread across others, emphasizing the need for WaTech to coordinate threat remediation efforts and implement safeguards that limit damage and accelerate service restoration.[2]

The prevalence of shadow IT (unauthorized or redundant technology systems) further complicates WaTech's security landscape by reducing visibility, introducing vulnerabilities, and weakening enterprise security standards. To address these challenges and meet future demands, WaTech's business goal is to establish a clear, actionable plan for aligning with and adopting a zero trust security framework.

Key business objectives included securing sponsorship from WaTech executive stakeholders, namely WaTech's Director and the state CIO, State CISO (SOC Management), State CTO (Enterprise Architecture), Chief Data Officer (CDO), Chief Privacy Officer, and the Deputy Director for Enterprise Technology Services. Additionally, WaTech is working to shift the perception of cybersecurity from a business inhibitor to a strategic enabler while aligning zero trust principles with the organization's overarching enterprise goals.

Introduction or Problem Statement

Imagine a security model where every access request is treated with the same level of scrutiny, regardless of its origin; whether inside or outside the network. That concept encapsulates zero trust. By implementing zero trust, an organization ensures that every user, device, and application is continuously verified, and access is granted strictly based on roles and responsibilities.

[1] RCW 43.105.450: Office of cybersecurity—State chief information security officer—State agency information technology security. https://app.leg.wa.gov/RCW/default.aspx?cite=43.105.450.
[2] Security Service Edge (SSE) Onboarding Project | WATECH. https://watech.wa.gov/security-service-edge-sse-onboarding-project.

A zero trust approach not only strengthens protection against cyber threats but also mitigates potential damage resulting from breaches. Zero trust represents a smart, modern strategy to help enterprises remain resilient and agile amidst evolving security challenges.

In today's rapidly changing digital landscape, organizations encounter increasingly sophisticated cyber threats capable of compromising sensitive data and disrupting operations. Traditional perimeter-based security models are no longer adequate. To address these challenges, adopting a zero trust security framework is essential for securing digital assets**.**

Purpose of this document

The purpose of this document is to educate readers on the importance of zero trust in the digital age, where technology evolves rapidly, and malicious actors need only succeed once to compromise data, identities, and livelihoods. This zero trust white paper provides a comprehensive overview of the critical role zero trust plays, what it entails, where it fits within the broader security landscape, and how it can enhance the protection of data, systems, infrastructure, and users pertaining to Washington State Government.

Business Justification for Zero Trust

Zero trust is a security framework that operates on the principle of "never trust, always verify." Adopting zero trust aligns security with business goals, ensuring resilience against evolving threats while supporting operational agility.

Who should care about zero trust?

CIOs and CISOs

Zero trust encompasses most of the National Association of State Chief Information Officers (NASCIO 2025) priorities, the goals of the state's Enterprise IT Strategic Plan, and other mandates.[3] [4]

- Zero trust is the cornerstone to revolutionize the cybersecurity and risk management governance, practices, and capabilities of the state enterprise (NASCIO 2025 1st priority and the purpose of WaTech's Office of Cybersecurity).[5]
- Zero trust enables adoption of artificial intelligence and machine learning automation (NASCIO 2nd priority, Enterprise Strategic Goal #3, and gubernatorial Executive Order).[6]
- Zero trust will improve a user's experience with the state government's digital services (NASCIO 3rd priority and Enterprise Strategic Goal #4).
- Zero trust is the approach that will protect state data and deliver analytics to enable data-driven decisions to be rendered (NASCIO 4th priority and Enterprise Strategic Goal #2).

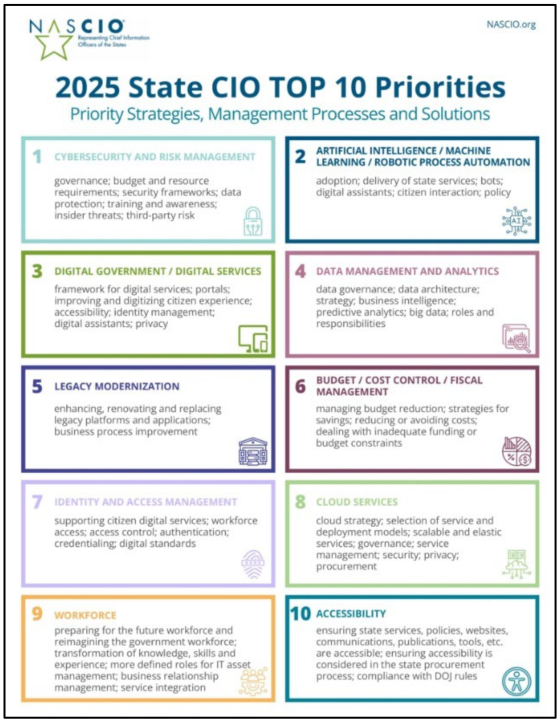
[3] *State CIO Top Ten Policy and Technology Priorities for 2025 - NASCIO. https://www.nascio.org/wp-content/uploads/2024/12/NASCIO-2025-State-CIO-Top-10-Priorities_a11y.pdf*

[4] *Enterprise IT Strategic Plan | WATECH. (n.d.). https://watech.wa.gov/strategy/enterprise-it-strategic-plan*

[5] *Chapter 43.105 RCW: WASHINGTON TECHNOLOGY SOLUTIONS*. (n.d.). https://app.leg.wa.gov/rcw/default.aspx?cite=43.105&full=true#43.105.450

[6] (n.d.). Governor Jay Inslee. https://governor.wa.gov/sites/default/files/exe_order/24-01%20-%20Artificial%20Intelligence%20%28tmp%29.pdf

- Zero trust bridges the evolution of legacy modernization (NASCIO 5th priority and Enterprise Strategic Goal #2).
- Zero trust can reduce technology sprawl by unifying architectural lifecycle practices in the same strategic direction (NASCIO 6th priority and Enterprise Strategic Goal #2).
- Zero trust Identity and Access Management (IAM) is the key cornerstone around how an organization leverages Zero Trust Architecture (ZTA) to reach the goal of ZTNA (NASCIO 7th priority).[7]
- Zero trust will allow organizations to safely adopt cloud IT services (NASCIO's 8th priority and enables the State Cloud Smart Strategy).[8]
- Zero trust will allow the state's workforce to evolve into an innovative culture transforming how we work together (NASCIO 9th priority and Enterprise Strategic Goal #4).
- Zero trust enables the safe expansion of broadband Internet and wireless connectivity (NASCIO 10th priority and promotes the goals of the State's Broadband Initiative).[9]
- Leaders responsible for IT and security should prioritize zero trust to protect their organizations from evolving threats.



NASCIO
Representing Chief Information Officers of the States

NASCIO.org

2025 State CIO TOP 10 Priorities

Priority Strategies, Management Processes and Solutions

1 CYBERSECURITY AND RISK MANAGEMENT
governance; budget and resource requirements; security frameworks; data protection; training and awareness; insider threats; third-party risk

2 ARTIFICIAL INTELLIGENCE / MACHINE LEARNING / ROBOTIC PROCESS AUTOMATION
adoption; delivery of state services; bots; digital assistants; citizen interaction; policy

3 DIGITAL GOVERNMENT / DIGITAL SERVICES
framework for digital services; portals; improving and digitizing citizen experience; accessibility; identity management; digital assistants; privacy

4 DATA MANAGEMENT AND ANALYTICS
data governance; data architecture; strategy; business intelligence; predictive analytics; big data; roles and responsibilities

5 LEGACY MODERNIZATION
enhancing, renovating and replacing legacy platforms and applications; business process improvement

6 BUDGET / COST CONTROL / FISCAL MANAGEMENT
managing budget reduction; strategies for savings; reducing or avoiding costs; dealing with inadequate funding or budget constraints

7 IDENTITY AND ACCESS MANAGEMENT
supporting citizen digital services; workforce access; access control; authentication; credentialing; digital standards

8 CLOUD SERVICES
cloud strategy; selection of service and deployment models; scalable and elastic services; governance; service management; security; privacy; procurement

9 WORKFORCE
preparing for the future workforce and reimagining the government workforce; transformation of knowledge, skills and experience; more defined roles for IT asset management; business relationship management; service integration

10 ACCESSIBILITY
ensuring state services, policies, websites, communications, publications, tools, etc. are accessible; ensuring accessibility is considered in the state procurement process; compliance with DOJ rules

The figure above illustrates NASCIO's Top Ten Policy and Technology Priorities for 2025.[10]

[7] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. *Zero Trust Architecture*, *800-207*(800-207). https://doi.org/10.6028/nist.sp.800-207

[8] *State Cloud Smart Strategy -DRAFT*. (2023). https://watech.wa.gov/sites/default/files/2023-11/State%20of%20Washington%20Cloud%20Strategy%201.0%20Published.pdf

[9] *RCW 43.330.532: Broadband office—Established—Purpose.* (2019). Wa.gov. https://app.leg.wa.gov/RCW/default.aspx?cite=43.330.532

[10] *NASCIO.org. (n.d.). 2025 State CIO TOP 10 Priorities. https://www.nascio.org/wp-content/uploads/2024/12/NASCIO-2025-State-CIO-Top-10-Priorities_a11y.pdf*

IT Departments

Technical teams need to implement and manage zero trust architectures to secure networks and systems effectively.

Compliance Officers

Those responsible for regulatory compliance will find zero trust frameworks helpful in meeting security and data protection standards.

Data Protection Officers

Individuals tasked with protecting sensitive information can leverage zero trust principles to enforce stricter access controls.

Business Leaders and Executives

As breaches can lead to significant financial loss and reputational damage, leaders should understand the importance of robust security frameworks like zero trust.

Employees (the workforce)

Everyone in the organization plays a critical role in security; understanding zero trust can help employees follow best practices in data handling and access.

Business Justification

Adopting a zero-trust security model is essential for several business reasons.

- **Evolving Threat Landscape**
  - Cyber threats are increasingly sophisticated. Zero trust mitigates risks by assuming that threats can come from both outside and inside the organization, ensuring robust defenses against breaches.
  - Please refer to Appendix 1 – Threat Landscape Context for additional details about the cybersecurity threats that zero trust can address or mitigate.
- **Data Protection**
  - With sensitive data scattered across multiple locations (cloud, on-premises, hybrid or collaboration etc.), zero trust helps safeguard this information through strict access controls, minimizing the risk of data leaks.
- **Adaptation to Remote Work (Remote Work Enablement)**
  - As remote work becomes the norm, zero trust ensures secure access to corporate resources regardless of location, providing flexibility while maintaining security.
- **Least Privilege Access**
  - Implementing zero trust encourages the principle of least privilege, granting users only the access they need. This limits potential damage from compromised accounts.

- **Regulatory Compliance**
  - Many industries face stringent regulatory requirements regarding data protection. Zero trust can help organizations meet compliance mandates by enforcing strict access and monitoring protocols.
- **Enhanced Visibility and Monitoring**
  - Zero trust frameworks often include continuous monitoring and analytics, providing greater visibility into digital behaviors and potential anomalies, enabling faster threat detection and response. Continuous monitoring and logging are integral to zero trust, allowing organizations to quickly detect and respond to suspicious activity.
- **Agility and Resilience**
  - With a ZTA, organizations can adapt more quickly to changing business needs and emerging threats, fostering resilience in the face of cyber incidents.[11]
- **Reduced Attack Surface**
  - By enforcing strict access controls and continuous verification, zero trust limits the potential points of ingress and egress for threat actors.
- **Improved Incident Response**
  - By continuously validating user identities and device health, zero trust can streamline incident response processes, allowing for quicker identification and remediation of threats.
- **Legacy Systems**
  - Zero trust can provide security mitigations for legacy systems that might not support modern security protocols.

In summary, adopting a zero trust model is not just a technological shift but a strategic imperative that enhances security posture, protects critical assets, and supports the organization's overall resilience in an increasingly complex digital landscape.

[11] *Zero Trust Architecture: Strategies and Benefits | Gartner*. (2024). Gartner. https://www.gartner.com/en/cybersecurity/topics/zero-trust-architecture

Zero Trust Use Cases

Zero trust uses a combination of a modern enhanced security posture, that readily adapts to ever changing threat environment while maintaining regulatory compliance with industry standards. Zero trust utilizes continuous multi-factor authentication, micro-segmentation, advanced encryption, enhanced endpoint security, robust data analytics and auditing, among other capabilities, to fortify data, applications, assets, and services to deliver cyber resiliency as part of a defense-in-depth strategy.

Zero trust has numerous benefits and use cases that are applicable to organizations.

- **Enhanced Security Posture:**
    - Reduces the risk of data breaches and other threats by limiting access and continuously validating user actions.
    - Segments security patterns and inspects traffic flows.
    - Improves data centric security protections, like encryption, access control, and continuous monitoring.
    - Improves access controls for cloud, multi-cloud, and container environments.
    - Secures remote connections, by limiting access and isolating Internet of Things (IoT) devices.
    - Creates a dynamic, adaptive policy feedback loop.
    - Improves security posture through real-time insight.
    - Ensures global uniform hygiene across all devices and restricts access to those that do not meet the standard.
    - Offers real-time dynamic, continuous authentication through contextual data.
    - Provides conditional authorization based on specific criteria like user roles and login origination.
- **Regulatory Compliance:**
    - Assists organizations in meeting compliance requirements by ensuring robust data protection measures.
    - Centralizes orchestration and policy management.
    - Supports organizational compliance initiatives.
- **Adaptability:**
    - Offers flexibility to support remote work and cloud environments, making it suitable for modern enterprise needs.
    - Securely supports remote users (telecommuting workforce).
    - Increases onboarding for new employees, third parties, and contractors.
    - Can entirely or partially replace the need for Virtual Private Networks (VPNs).

Please refer to Appendix 2 – Zero Trust Case Studies about why and how other organizations have adopted a zero-trust cybersecurity approach.

Zero Trust Challenges

Adopting a zero trust framework involves addressing several challenges.

1. **Cultural Resistance:** Shifting from traditional security mindsets to a zero trust approach can meet resistance from employees who may view it as overly restrictive or complex.
    a. An organization will need to formulate an effective marketing campaign to evangelize why zero trust is so important to alter its culture and the way its employees approach zero trust.
    b. An organization should evolve from an outside-in to inside-out security design approach (mentality).
    c. An organization should consider technology gaps as business opportunities.
    d. Please refer to Appendix 3 – Zero Trust Misconceptions for details about the myths of zero trust.
2. **Implementation Complexity:** Deploying zero trust requires significant changes to existing infrastructure, which can be complex and resource intensive.
    a. Organizations should implement zero trust incrementally, starting with high-risk areas, to manage complexity and resource allocation effectively.
    b. An organization should leverage framework standards to reduce the complexity of implementing zero trust. Some of the frameworks that can assist with planning for and operationalizing zero trust include the following.
        i. National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).[12]
        ii. NIST Risk Management Framework (RMF).[13]
        iii. NIST Security and Privacy Controls for Information Systems and Organizations (SPC-ISO).[14]
        iv. Center of Internet Security (CIS) Critical Security Controls.[15]
        v. Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model (ZTMM).[16]
        vi. Gartner's Secure Access Service Edge (SASE) Framework.[17]
        vii. Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM).[18]
    c. An organization should continue to leverage existing investments and balance priorities as zero trust capabilities are introduced.

[12] NIST. (2024). *Cybersecurity Framework*. National Institute of Standards and Technology. https://www.nist.gov/cyberframework

[13] NIST. (2016, November 30). *NIST Risk Management Framework*. NIST. https://csrc.nist.gov/projects/risk-management/about-rmf

[14] National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations. *Security and Privacy Controls for Information Systems and Organizations*, *5*(5). https://doi.org/10.6028/nist.sp.800-53r5

[15] Center for Internet Security. (2023). *CIS Critical Security Controls*. CIS. https://www.cisecurity.org/controls

[16] CISA. (2023). *Zero Trust Maturity Model*. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

[17] *Definition of Secure Access Service Edge (SASE) - Gartner Information Technology Glossary*. (n.d.). Gartner. https://www.gartner.com/en/information-technology/glossary/secure-access-service-edge-sase

[18] *Cloud Security Alliance*. (n.d.). Cloud Security Alliance. https://cloudsecurityalliance.org/research/cloud-controls-matrix

3. **Legacy Systems Integration:** Many organizations rely on outdated systems that may not support zero trust principles, complicating integration efforts.
    a. Organizations will be challenged with integrating existing security tools with new technologies to harmonize their digital ecosystem.
    b. An organization should leverage ZTA to integrate existing systems with new technologies (blending technology).[19]
    c. An organization should integrate Commercial and Government off-the-shelf (COTS/GOTS) solutions with existing systems.
    d. Replacing legacy systems that cannot integrate with new architecture should be replaced.
4. **Resource Allocation:** Adequate investment in technology and personnel is necessary, which can be a barrier for organizations with limited budgets.
    a. Organizations should leverage their centralized IT service provider or (central IT organization) to assist with zero trust planning.
    b. Organizations should tie zero trust investments to measurable security improvements, such as reduced breach risks and mitigation of threat vectors to justify expenditures.
    c. Organizations should consolidate overlapping tools and processes to streamline operations and reduce unnecessary spending.
5. **User Experience:** Striking a balance between security measures and user convenience is crucial; overly stringent or improperly implemented access controls can hinder productivity.
    a. Organizations should ensure that sufficient resource bandwidth is available to businesses to investigate, adopt and continuously support zero trust.
    b. An organization should leverage a single ticket management system to track and manage ticket volumes and staff workloads.
    c. Organizations should ensure clear communication with all affected parties during implementation and additional effort should be made to train users in the changes being made.
    d. Organizations should be clear in the message that zero trust is beneficial to them, the end user, and protects them and their data from loss or compromise.
6. **Continuous Monitoring and Maintenance:** Maintaining real-time monitoring and adapting to new threats requires ongoing resources and expertise.
    a. Organizations should invest in sufficient security staff and technology infrastructure to support proactive threat detection, mitigation, and system updates.
    b. Continuous monitoring and inspection of data flows should be implemented to detect anomalous activity and maintain security throughout the network.
    c. A unified monitoring dashboard can help consolidate security insights and streamline response efforts, reducing the risk of oversight.

[19] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. *Zero Trust Architecture*, *800-207*(800-207). https://doi.org/10.6028/nist.sp.800-207

   d. Organizations must be prepared to handle the log information and have a plan for what to do with the new information gained from implementing zero trust capable solutions.

7. **Data Privacy Concerns:** Implementing stringent access controls may raise concerns about data privacy and compliance with regulations.
   a. Organizations should incorporate applicable data compliance constraints and privacy objectives into a zero trust strategy to address these data privacy concerns.
   b. Organizations should ensure that access controls align with relevant data protection laws and frameworks.
8. **Skill Gaps:** A shortage of cybersecurity professionals with zero trust expertise can hinder effective implementation and management.
   a. An organization should foster a security-first philosophy through training and awareness programs to address the universal lack of understanding in zero trust, least privilege and SASE.[20]
   b. Organizations should ensure their teams have the expertise to conduct forensic investigations when needed.
9. **Vendor Lock-In:** Relying on specific technologies or vendors can create challenges with flexibility and adaptability in a rapidly evolving threat landscape.
   a. Organizations should leverage ZTA to effectively blend old and new infrastructure together.[21]
   b. Organizations should adopt a multi-vendor strategy to avoid dependency on a single provider and ensure they can switch solutions if needed.
   c. Regular assessments of vendor performance and the organization's security needs should be conducted to ensure the chosen technologies remain effective and scalable.
10. **Scalability:** As organizations grow, maintaining a scalable security posture while ensuring consistent security can be difficult.
    a. An organization should leverage CISA's ZTMM to accurately assess its capabilities to properly gauge its zero-trust maturity.[22]
    b. Organizations should design a flexible architecture from the outset, ensuring that security policies and controls can scale with the organization's growth.

Addressing these challenges requires careful planning, strong leadership commitment, and ongoing education to foster a security-first culture. The journey to zero trust is a gradual, evolving process that demands continuous adaptation and refinement as security needs and technologies change, ensuring a robust and resilient framework for the future.

[20] *Definition of Secure Access Service Edge (SASE) - Gartner Information Technology Glossary*. (n.d.). Gartner. https://www.gartner.com/en/information-technology/glossary/secure-access-service-edge-sase

[21] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. *Zero Trust Architecture*, *800-207*(800-207). https://doi.org/10.6028/nist.sp.800-207

[22] CISA. (2023). *Zero Trust Maturity Model*. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

Zero Trust Model

The Zero Trust Model is based on three concepts.

- **Assume Breach –**
  - In today's digital climate, organizations must assume that any component can (and may) be compromised, including monitoring and security tools used to protect against threat actors. Every access request is treated as a potential threat, requiring strict and strong authentication and authorization.
- **No Implicit Trust –**
  - Anyone on any computing device can compromise an IT system, exploit data, or disrupt a business service. Every attempt to access an organizational resource (devices, files, records, tables, directories, databases, mini-disks, processes, programs, domains) is treated as if the communication traffic flow is coming from an untrusted source (explicitly denied by default). In summary, never trust anyone or anything; always verify.
- **Continuous Verification –**
  - Authentication is not just a one-time process and should be subject to ongoing validation to continuously monitor data security patterns (traffic analytics), device status (usage, health), and user behaviors. All traffic going to and from a zero trust network (referred to as a protect surface) is subject to rigorous verification (inspected and logged) for malicious content and unauthorized activity, up through Layer 7. In summary: continuously verify everyone (users) and everything (devices) regardless of where a user or device is connecting from.

Pillars of Zero Trust

The pillars of a framework are the bedrock components of a functioning IT framework. CISA[23] has identified eight functional areas, consisting of five pillars and three supporting layers, that are the primary ingredients necessary to adopt (aligning with) zero trust.

Five of these functional areas form the pillars of zero trust:

1. **Identity (users)**

   An identity refers to an attribute (or set of attributes) that uniquely describes an organizational user or entity, including non-person entities.

2. **Devices (system health)**

   A device refers to any asset that can connect to a network, including servers, virtual machines/containers, desktops and laptops, printers, mobile phones, IoT and Industrial Internet of Things (IIoT) devices, networking equipment, and more.

3. **Network (organizational environment)**

   A network refers to an open communications medium including typical channels such as organizational internal networks, wireless networks, and the Internet as well as other potential channels such as cellular and application-level channels used to transport messages.

[23] Cybersecurity & Infrastructure Security Agency. (2020). *Homepage | CISA*. Cisa.gov. https://www.cisa.gov/

4. **Applications and Workloads**

   Applications and workloads include computing operating systems, computer programs, and services that execute on-premises, on mobile devices, and in cloud environments.

5. **Data (privacy, repositories)**

   Data refers to any digital information that is created, accessed, processed, stored, or transmitted within systems, devices, networks, applications, databases, infrastructure, and backups (including on-premises and virtual environments) as well as the associated metadata.

Below are the three supporting layers which span across all five pillars.

6. **Visibility and Analytics**

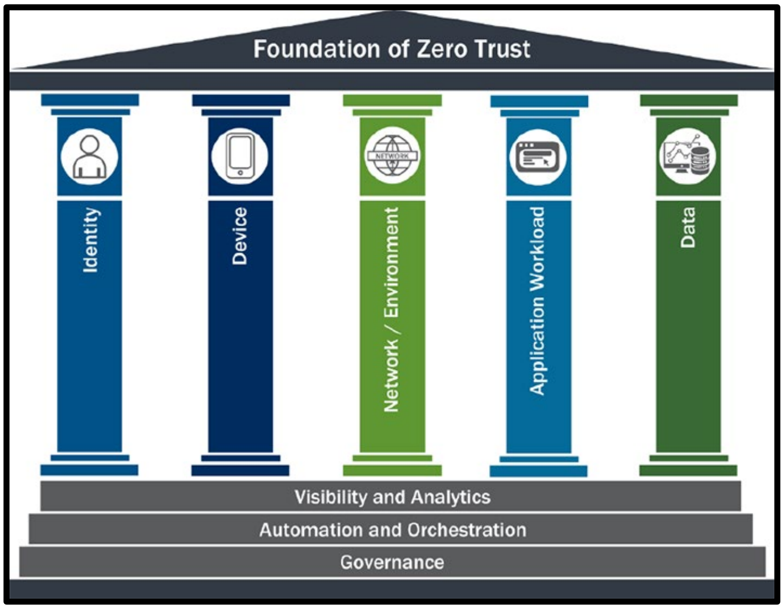
   Insights into activities across all pillars, ensuring that threats can be detected and addressed in real time.

7. **Automation and Orchestration**

   Enforces security policies across all pillars, ensuring that security measures are consistently applied with minimal [manual] intervention.

8. **Governance**

   Provides overarching policies and frameworks that ensure the entire zero trust strategy is compliant with regulations and aligned with organizational objectives.



The figure above illustrates the relationship between the eight functional areas which form the foundation of zero trust.[24]

[24] Team, E. E. (2021, October 26). *Incorporating VMware Zero-Trust for the Presidential Executive Order*. VMware End-User Computing Blog. https://blogs.vmware.com/euc/2021/10/incorporating-vmware-zero-trust-for-the-presidential-executive-order.html

Zero Trust Principles

Zero trust principles are rules, concepts, or beliefs that guide an organization towards zero trust. There are common principles that are consistent that guide an organization towards zero trust. [25] [26] [27] [28]

- **Least Privilege Access –**
  - The notion of enabling the minimum level of access that a device or user requires.
  - Determine who or what needs access to a resource.
    - It is common for organizations to give users more access than what is required for their assigned duties.
    - Organizations should determine who needs to have access to a resource or asset to complete their job so that access to resources is limited to a need-to-know basis.
    - Multi-Factor Authentication (MFA) and other advanced methods are used to ensure that only authorized users and devices can access sensitive resources.
  - Identity-centric governance (based on identity and assigned attributes).
    - Users should only be granted the minimum level of access necessary to perform their duties based on their role.
    - Devices should meet specific security requirements (such as up-to-date antivirus or encryption) before being allowed to access critical applications. Access should depend on the security state of the device making the request.
    - Application accessibility should be approved based on the sensitivity of the application itself. Critical or highly sensitive applications may require stricter access controls compared to less sensitive ones.
    - This means even if a user, application, or device is compromised, the potential damage is limited by restricting what the threat actor can access and exploit.
  - Contextual Access Control.
    - Access controls should evaluate a resource's access based on a variety of factors to include, but not limited to user identity, device status, location, and behavior (UEBA).
  - In summary: limit access based on absolute business need with a robust Identity and Access Management (IAM) strategy based on zero trust.

[25] Implementing Zero Trust Security in the Public Sector. Gartner. (n.d.). https://www.gartner.com/en/industries/government-public-sector/topics/zero-trust

[26] DoD Zero Trust Strategy. (November 7, 2022). Department of Defense https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

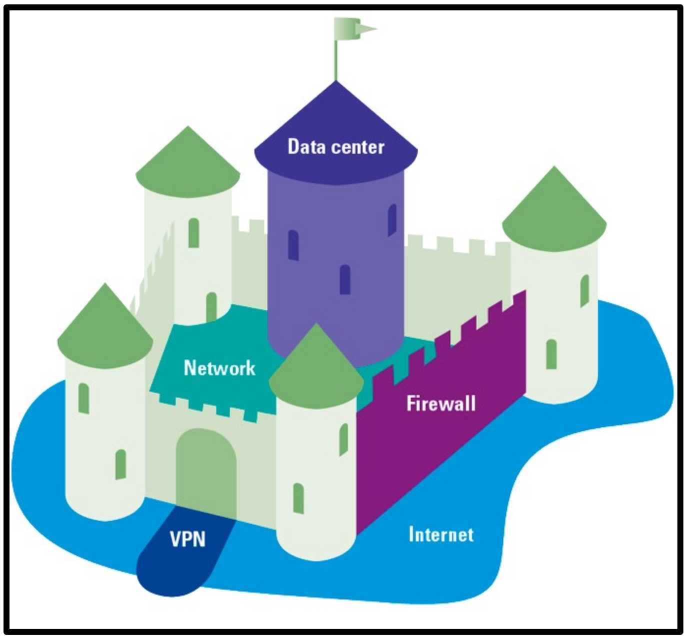
[27] Zero Trust Architecture. (August 2020). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[28] Zero Trust Maturity Model 2.0. (April 2023). Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf

- **Segmentation –**
  - A goal of zero trust is to mitigate the business impact (i.e., limit the blast radius) of a cybersecurity event by preventing lateral movement within a digital ecosystem while controlling access to corporate data.
  - Segmentation involves emplacing micro-perimeters around specific data or assets so that more granular technical controls can be implemented, and technical policy can be enforced.
    - i.e., Segmentation means placing small boundaries around specific data or assets to apply detailed technical controls and enforce policies more effectively.
  - A zero trust network is segmented into smaller, isolated zones to limit lateral movement within the network. Constraining lateral movement within a network means that even if an attacker gains access to one part of the network, the attacker will find it difficult to move to other areas.
    - This also includes networks constraining connectivity to the least function principle and a transition toward service-specific interconnections.
  - A combination of macro and micro-segmentation controls should be emplaced to properly segment an entire digital ecosystem.
- **Automation –**
  - Zero trust involves continuously monitoring computing resource usage, health, and analytics.
  - Policy Enforcement: Access control policies should be dynamically enforced based on the user's role, device posture, location, and other contextual factors.
    - Automated policies should adapt in real-time based on evolving threats and operational changes.
  - Machine learning and artificial intelligence capabilities should be leveraged to mitigate manual intervention.
- **Begin with end state in mind –**
  - Avoid 'putting the cart before the horse' by determining the 'why' and then the 'what' followed by the 'how'. Too many times, designers want to jump into designing before understanding why and what they are designing.
    - **WHY:** Why does an organization need zero trust?
    - **WHAT**: What are the expected outcomes and the organizational goals and objectives of zero trust?
    - **HOW**: How is an organization going to align with and adopt zero trust?
  - In summary: Focus on business solutions and less on technical designs.
- **Don't overcomplicate zero trust –**
  - Avoid overthinking; Keep It Simple, Stupid (the K.I.S.S. approach). Incorporate zero trust language, avoid establishing unique or new definitions for established zero trust terminology. Use plain talk to communicate zero trust to the lowest common denominator.
  - In summary: refrain from convoluting the concept of zero trust.

Traditional Design Methodology

- Traditional security models that rely heavily on perimeter defenses; assuming that everything inside the network is trustworthy and everything outside is not.
- Trust is assumed.[29]
    - The old saying: “Trust but verify” is no longer sufficient and should not be referred to due to today’s threat landscape.[30] [31]
- Outside-in approach: Security safeguards are focused on perimeter defense.
- System access decisions are static binary.
    - IAM is functional but basic.
- Default security mentality is to protect everything.
    - This mentality is no longer feasible due to budgeting, resourcing, competencies, and political constraints. A security team must be effective all the time when a hacker only must be effective once.
- Security and networking activities are manual (not dynamic) and reactive (not proactive).



The figure above shows how the traditional IT domains are organized.[32]

[29] Implementing Zero Trust Security in the Public Sector. Gartner. (n.d.). https://www.gartner.com/en/industries/government-public-sector/topics/zero-trust

[30] DoD Zero Trust Strategy. (November 7, 2022). Department of Defense https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[31] Zero Trust Architecture. (August 2020). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[32] Outdated “castle-moat” cyber defense setup. (August 2020). Compact Magazine. https://www.compact.nl/articles/zero-trust-beyond-the-hype/

Zero Trust Design Methodology

In essence, zero trust shifts the focus from perimeter-based security to a more granular and dynamic approach. Zero trust acknowledges that the traditional network boundary is no longer sufficient to protect against threats and that a more comprehensive strategy is required to safeguard critical assets. The following design principles of zero trust are incorporated when developing a zero trust design.

- **Trust nothing (assume breach)**
    - Verify everyone (users), and everything (devices and applications); authorization is explicit and based on roles and responsibilities.
    - Adopt advanced IAM practices involving the use of Privileged Access Management (PAM).
- **Real-time (proactive) decision making**
    - Resource and asset access decisions are real-time (dynamic/automated), multifactorial, contextual, session-based, attribute-based, and risk-based (advanced MFA).
    - Cybersecurity landscape (industry) has shifted to focus more on response and recovery by limiting how much of our digital ecosystem can be exploited. Thus, reducing the attack footprint.
    - The mentality now is to mitigate and remediate security events as fast as possible while further exploitation is minimized or stopped.
- **Zero trust is designed from the inside-out**
    - Adopt privacy and security by design methodology; focus on data defense and strategically defined perimeters. [33] [34] [35]
    - A good rule-of-thumb in design is to place the controls as close as possible to a protect surface.[36]
    - Start with organizational Data, Assets, Applications, and Services (DAAS) elements and the protect surfaces that need safeguarding and design outward from there.[37]
        - Leverage CSA's Defining the Zero Trust Protect Surface guidance to quickly and properly identify and confirm your protect surface(s).[38]
        - Use Info-Tech's Zero Trust Protect Surface Mapping Tool to identify key protect surfaces and map them to business goals.[39]

[33] *Secure by Design, Secure by Default | CISA. (n.d.). www.cisa.gov. https://www.cisa.gov/securebydesign*

[34] Build a Zero Trust Roadmap. Info-Tech. (n.d.). https://www.infotech.com/research/ss/build-a-zero-trust-roadmap

[35] Implementing Zero Trust Security in the Public Sector. Gartner. (n.d.). https://www.gartner.com/en/industries/government-public-sector/topics/zero-trust

[36] Kindervag J. Define a protect surface to massively reduce your attack surface. *Palo Alto Networks Blog*. May 2019. https://www.paloaltonetworks.com/blog/2018/09/define-protect-surface-massively-reduce-attack-surface/.

[37] Department of Defense. *Zero Trust Overlays*.; 2024. https://dodcio.defense.gov/Portals/0/Documents/Library/ZeroTrustOverlays.pdf?

[38] *Defining the Zero Trust Protect Surface* | *CSA*. (2024). Cloudsecurityalliance.org. https://cloudsecurityalliance.org/artifacts/defining-the-zero-trust-protect-surface

[39] Info-Tech Research Group. Zero Trust Protect Surface mapping tool. Info-Tech Research Group. https://www.infotech.com/research/zero-trust-protect-surface-mapping-tool.

    - If/as needed, an organization could leverage the (CIS) Network and Web Application Vulnerability Assessment service to discover and map an organization’s network, discover organizational assets, identify network and web application vulnerabilities, prioritize vulnerability remediation, and provide remediation tracking according to business risk.[40] [41]

- **Protect critical DAAS**
  - **Data** – Sensitive data that poses the greatest risk if exfiltrated or misused (i.e., what data must be protected and where is that data). Defining the protect surface entails identifying, categorizing, and assessing an organization's DAAS. Protect surfaces will influence organizational risk and advise zero trust maturity.
    - Examples include PCI Data Security Standard (PCI DSS)[42], HIPAA Privacy Rule[43], Federal Tax Information Security Guidelines (Pub 1075)[44], Personally Identifiable Information (PII)[45], and Intellectual Property (IP)[46].
    - In the state government context, data will fall into one of four data categories.
      - State data categories are 1, 2, 3, 4.
      - Please refer to WaTech’s Categorizing Data for a State Agency on how to categorize state data.[47]
      - Additional guidance of categorizing state data can be obtained from the state’s Data Classification Standard.[48]
    - Since data is a primary cornerstone pertaining to zero trust, this makes the Chief Data Officer (CDO) a critical stakeholder.
    - Agencies can use the following guidance to help define and identify your organizational protect surfaces.
    - Outcome: to clearly identify what will be protected and why so that administrative policy can shape technical access controls and criteria can be developed to account for full versus partial access to organizational DAAS.
  - **Assets** – Critical physical or virtual devices and systems that store, process, or transmit sensitive data; this includes IT, Operational Technology, and the IoT that are essential to business operations.
    - Examples include servers, workstations, endpoints, networking devices, storage arrays, and networked devices.

[40] *Vulnerability Assessments*. (2021, October). CIS. https://www.cisecurity.org/services/vulnerability-assessments

[41] Center of Internet Security (CIS). (2018). CIS. https://www.cisecurity.org/

[42] PCI Security Standards Council. (n.d.). *PCI Data Security Standard (PCI DSS)*. PCI Security Standards Council. https://www.pcisecuritystandards.org/standards/pci-dss/

[43] *SUMMARY OF THE HIPAA PRIVACY RULE HIPAA Compliance Assistance. (2003). https://www.hhs.gov/sites/default/files/privacysummary.pdf*

[44] Bannister Patricia I, & OS:P:GLDS:S. (2016). *Publication 1075 Tax Information Security Guidelines For Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns and Return Information*. https://www.irs.gov/pub/irs-pdf/p1075.pdf

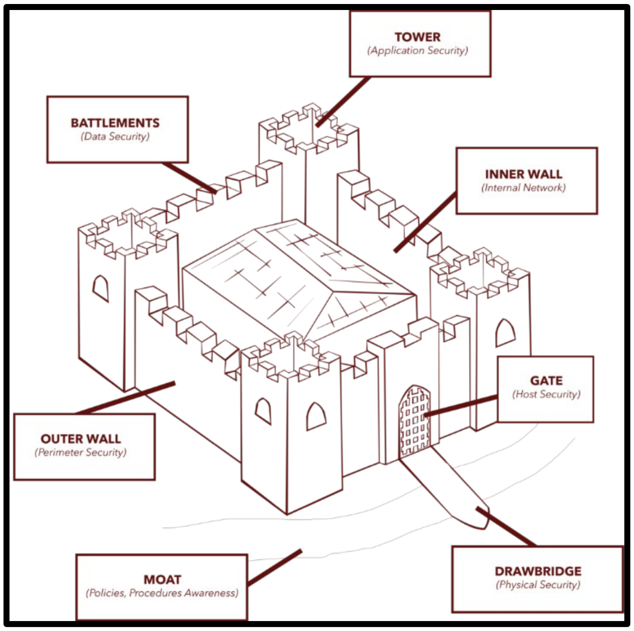
[45] Editor, C. C. (n.d.). *Personally Identifiable Information (PII) - Glossary | CSRC*. Csrc.nist.gov. https://csrc.nist.gov/glossary/term/personally_identifiable_information

[46] Editor, C. C. (n.d.). *Intellectual Property - Glossary | CSRC*. Csrc.nist.gov. https://csrc.nist.gov/glossary/term/intellectual_property

[47] *Categorizing data for a state agency | WaTech*. (2022). Wa.gov. https://watech.wa.gov/categorizing-data-state-agency

[48] *DATA CLASSIFICATION STANDARD*. (2017). https://watech.wa.gov/sites/default/files/2024-09/SEC-08-01-S%20Data%20Classification%20Standard.pdf

- **Applications** – Software and firmware that use sensitive data or control critical assets.
  - Examples include a line of business applications, Enterprise Planning and Customer Relationship Management (ERP and CRM) software or other off-shelf software.
- **Services** – Foundational technologies that are crucial to the day-to-day operation of an organization.
  - Examples include the most common services that should be protected include Domain Name Services (DNS), DHCP, domain controllers, Active Directory (Entra ID), system timing, authentication mechanisms, and critical infrastructure that enables communication and data exchange.



The figure above illustrates the defense approach to designing zero trust solutions.[49]

In summary, zero trust will warrant Confidentiality, Integrity, and Availability (CIA) of organizational assets (data), resources (people), and services.[50]

[49] *Philosophy – Roman Data Defense*. (2021). Romandata.com. https://romandata.com/philosophy/

[50] *Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., Sweetnam, J., & Townsend, A. (2020, December). Executive Summary — NIST SP 1800-26 documentation. www.nccoe.nist.gov. https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html*

Zero Trust Architecture

NIST’s publication, Engineering of Trustworthy Secure Systems, should be used as a guide when developing design solutions and ensuring interoperability between legacy IT systems and new systems and architectures.[51]

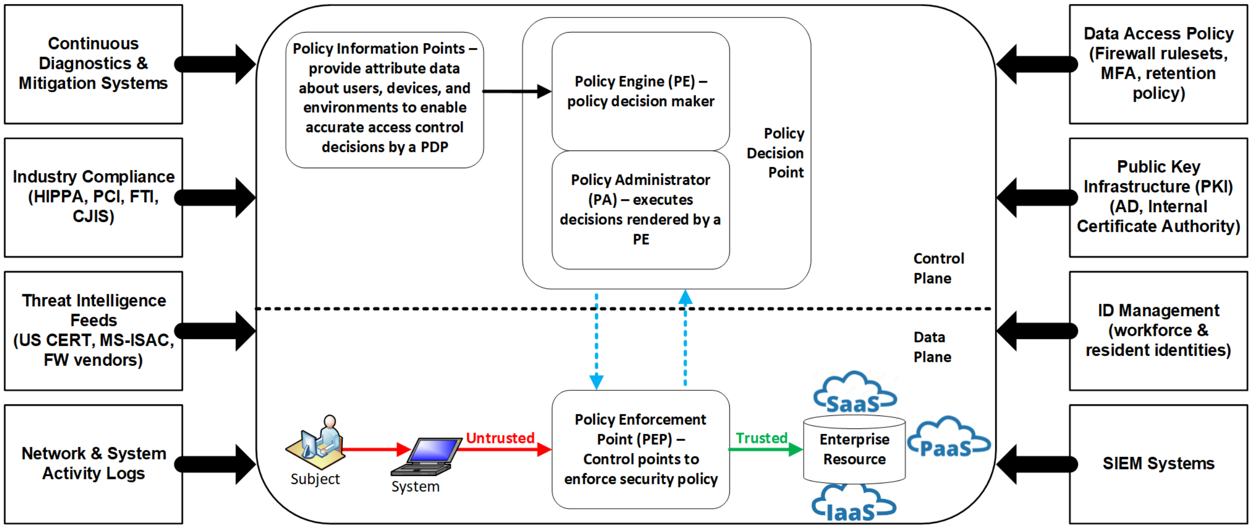
- Adopt security by design practices. Start with security in mind instead of later in the design process.[52]

Centralized vs. Decentralized Policy Enforcement – Zero trust centralizes policy decision-making for subjects (endpoints, users) which want to access policy information points (identity credentials, protected resources, analytics) or enterprise resources (applications, servers, cloud resources).

Zero trust assimilates ZTA, the capabilities inherent to a SASE framework, and zero trust capabilities into a unified strategy to directly support interconnecting branch office resiliency, remote workers, and on-premises.[53]

As endpoints initiate a request to confirm a user’s identity with an identity broker (like Entra ID), the request flows through a Policy Enforcement Point (PEP) which exchanges information with a Policy Decision Point (PDP) to confirm and authenticate a user’s identity credentials.

- A PDP inquires with a Policy Information Point (PIP) to authenticate a user while validating the resources which a user is authorized to access.


Continuous Diagnostics & Mitigation Systems
Industry Compliance (HIPPA, PCI, FTI, CJIS)
Threat Intelligence Feeds (US CERT, MS-ISAC, FW vendors)
Network & System Activity Logs
Policy Information Points – provide attribute data about users, devices, and environments to enable accurate access control decisions by a PDP
Policy Engine (PE) – policy decision maker
Policy Administrator (PA) – executes decisions rendered by a PE
Policy Decision Point
Control Plane
Data Plane
Subject
System
Untrusted
Policy Enforcement Point (PEP) – Control points to enforce security policy
Trusted
Enterprise Resource
SaaS
PaaS
IaaS
Data Access Policy (Firewall rulesets, MFA, retention policy)
Public Key Infrastructure (PKI) (AD, Internal Certificate Authority)
ID Management (workforce & resident identities)
SIEM Systems

The figure above illustrates the Core Zero Trust Logical Components which form ZTA.[54]

[51] Ross, R. S. (2022). *Engineering Trustworthy Secure Systems*. https://doi.org/10.6028/nist.sp.800-160v1r1

[52] *Secure by Design, Secure by Default | CISA*. (n.d.). Www.cisa.gov. https://www.cisa.gov/securebydesign

[53] *Definition of Secure Access Service Edge (SASE) - Gartner Information Technology Glossary*. (n.d.). Gartner. https://www.gartner.com/en/information-technology/glossary/secure-access-service-edge-sase

[54] Zero Trust Architecture: A Brief Introduction. *(n.d.). SSL.com. https://www.ssl.com/blogs/zero-trust-architecture-a-brief-introduction/*

ZT vs. ZTA vs. ZTNA

Zero Trust

- John Kindervag (the inventor of the Zero Trust Model) defines ZT as: "*A strategy designed to stop data breaches and prevent other cyber-attacks from being successful by eliminating trust from digital systems*."[55]
    - The CSA summarized NIST's ZT definition as a security framework that encompasses a structured approach to aligning with the concept of no implicit trust is granted (trust nothing; verify everything).[56] [57]
- NIST proclaims: "*Zero trust is a cybersecurity paradigm [model] focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated. Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised*."[58]
- ZT is a strategy (journey, plan, or approach); ZT is a set of granular allow rules.
- ZT frameworks include, but are not limited to: DoD ZT Strategy, NIST ZTA, CISA ZTMM, and Gartner SASE.

Zero Trust Architecture

- NIST defines ZTA as: "*an enterprise cybersecurity architecture that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement. ZTA uses ZT principles to plan industrial and enterprise infrastructure and workflows*."[59]
    - Furthermore, "*Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies*."[60]
- DoD summarizes ZTA as providing near real-time validation of devices to ensure compliance of [administrative and technical] policy at the time a device tries to access any resource.[61]

[55] *Win the CyberWar with Zero Trust*. (n.d.). https://www.sig-switzerland.ch/wp-content/uploads/2024/04/240411_John_Kindervag_Win_The_Cyberwar_With_Zero_Trust.pdf

[56] *Home. (n.d.). Cloud Security Alliance. https://cloudsecurityalliance.org/*

[57] *Zero Trust Maturity Model | CISA*. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/zero-trust-maturity-model

[58] *Zero Trust Maturity Model | CISA*. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/zero-trust-maturity-model

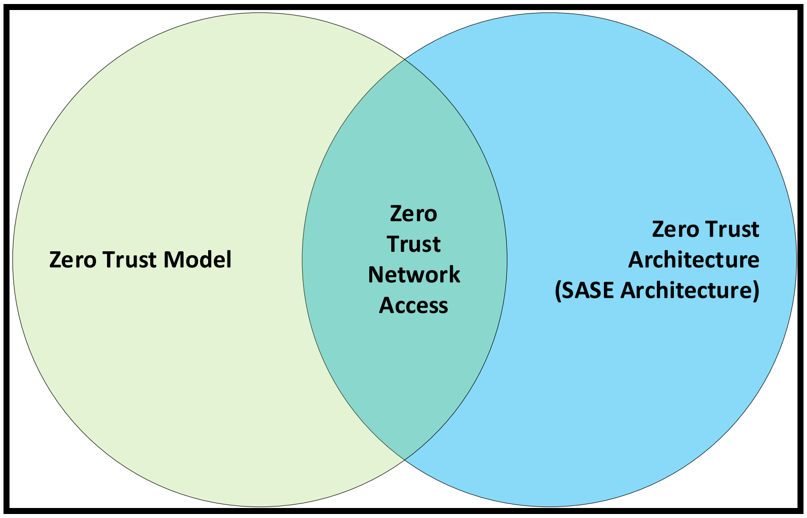
[59] Rose, S., Borchert, O., Mitchell, S., Connelly, S., National Institute of Standards and Technology, Advanced Network Technologies Division, Stu2Labs, & Cybersecurity & Infrastructure Security Agency. (2020). *Zero trust architecture*. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

[60] Rose S, Borchert O, Mitchell S, et al. *Zero Trust Architecture*.;
2020. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf.

[61] Department of Defense. *Zero Trust Overlays*.;
2024. https://dodcio.defense.gov/Portals/0/Documents/Library/ZeroTrustOverlays.pdf?

Zero Trust Network Access

- Gartner defines Zero Trust Network Access (ZTNA) as: "*a product or service that 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 trust broker* [ENTRA] *to a set of named entities. The broker* [ENTRA] *verifies the identity, context and policy adherence of the specified participants before allowing access and prohibits lateral movement elsewhere in the network. This removes application assets from public visibility and significantly reduces the surface area for attack.*"[62]
  - Note: the term 'application' can refer to SaaS or private applications (based on applicability).


Zero Trust Model
Zero Trust Network Access
Zero Trust Architecture (SASE Architecture)

The figure above shows the relationship between the Zero Trust Model and Zero Trust Architecture (inclusive of SASE Architecture) to achieve ZTNA.

ZT	ZTA	ZTNA
• Security strategy • Concept framework • Structured approach • No implicit trust • Least privileged • NIST, CISA, DoD aligned	• ZT Principle based • Component relationships • Workflow planning • Access policies • Preventing breaches • Limit lateral movement	• Trust broker • Identity/context-based accessibility • Conceal apps and users • Increase protect surfaces • ZT Foundation

[62] *Definition of Zero Trust Network Access (ZTNA) - Gartner Information Technology Glossary*. (n.d.). Gartner. https://www.gartner.com/en/information-technology/glossary/zero-trust-network-access-ztna-

In essence,

- Zero Trust (ZT) is the overarching cybersecurity model that assumes no one and nothing is trusted by default and access should always be verified and continuously monitored.
- ZTA is the framework or design for implementing zero trust principles across an organization's systems and infrastructure, including technologies like MFA, IAM, and micro-segmentation. ZTA is the hardware, software, and firmware that is coupled (blended) together to enable security patterns.[63]
- Zero Trust Network Access (ZTNA) is a specific technology or capability that provides secure, context-driven access to applications or resources, replacing traditional VPNs by verifying users and devices before granting access to specific resources. ZTNA[64] is the foundation of zero trust (per the CSA).[65]

Conclusion

As the digital landscape continues to evolve, so too must our approach to cybersecurity. The traditional perimeter-based security model is no longer sufficient to protect against increasingly sophisticated threats and the expanding attack surface brought on by cloud adoption, remote work, and interconnected systems.

Zero trust represents a fundamental shift in security philosophy; one that assumes no implicit trust and requires continuous verification of every user, device, and application accessing system resources. By implementing a zero trust architecture, organizations can significantly reduce risk, improve visibility, and enhance resilience against modern cyber threats while introducing automated capabilities for increased manageability.

Transitioning to zero trust is not a one-time project, but a journey and a mindset. Zero trust requires a strategic alignment of people, processes, and technologies, as well as executive commitment and cross-functional collaboration. An organization can align with a SASE Framework as a starting point to converge security and networking capabilities while zero trust principles, ZTA, and ZT decision-making is adopted. Organizations that invest in zero trust today will be better positioned to secure their digital assets, ensure regulatory compliance, and build a more robust and agile security posture for the future.

[63] *Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. Zero Trust Architecture, 800-207(800-207). https://doi.org/10.6028/nist.sp.800-207*

[64] *Definition of Zero Trust Network Access (ZTNA) - Gartner Information Technology Glossary*. (n.d.). Gartner. https://www.gartner.com/en/information-technology/glossary/zero-trust-network-access-ztna-

[65] *Home. (n.d.). Cloud Security Alliance. https://cloudsecurityalliance.org/*

Appendix 1 – Threat Landscape Context

The evolving cyber threat landscape underscores the urgent need for organizations to adopt a zero trust approach to security. Traditional perimeter-based defenses are no longer sufficient in an era of sophisticated cyberattacks, increasing reliance on cloud services, remote work, and the proliferation of connected devices. Zero trust addresses these challenges by shifting the focus from implicit trust to continuous verification of all users, devices, and data flows.

Ransomware Attacks – Ransomware remains one of the most prevalent and damaging cyber threats. Attackers exploit weak credentials, unpatched vulnerabilities, and phishing tactics to encrypt critical systems and demand ransom payments.

- Zero trust mitigates ransomware attacks by implementing micro-segmentation and least privilege access. For example, even if an attacker compromises a user's credentials, zero trust policies can limit lateral movement, preventing the spread of ransomware across systems.

Insider Threats – Malicious or negligent insiders continue to pose significant risks, with unauthorized access and data exfiltration being common attack vectors. Traditional defenses often fail to detect or mitigate such threats.

- Continuous monitoring and behavior analytics within a zero trust framework can detect abnormal activities, such as attempts to access unauthorized data, and automatically block these actions in real time.

Supply Chain Attacks – Attackers increasingly exploit vulnerabilities in third-party software or services to infiltrate organizations. These attacks can compromise entire ecosystems by targeting trusted partners or suppliers.

- Supply chain attacks are mitigated through strict access controls, continuous validation, and segmentation. By ensuring that third-party applications or services have limited and monitored access, zero trust reduces the likelihood of a supplier compromise affecting broader systems.

Phishing and Social Engineering – Phishing and social engineering remain effective methods for attackers to gain access, as users unknowingly divulge sensitive information or download malicious content.

Advanced Persistent Threats (APTs) – APTs are targeted attacks by well-funded adversaries who maintain a foothold in a network for extended periods, exfiltrating data or sabotaging systems.

- Continuous monitoring and AI-driven anomaly detection within a zero trust framework can uncover and disrupt APT activities before significant damage occurs, even if the attackers gain initial access. Additionally, principles like Zero Standing Privileges (ZSP) and enforcing strict access controls can increase detection of APTs or eliminate their foothold by requiring the threat actor to re-authenticate.

IoT and OT Vulnerabilities – The rapid adoption of Internet of Things (IoT) and Operational Technology (OT) devices has expanded the attack surface, often exposing critical infrastructure to cyber risks.

- In industrial environments, zero trust can isolate IoT and OT devices, limiting access to only essential systems. For example, a compromised IoT sensor cannot be leveraged to attack critical infrastructure due to micro-segmentation.

Cloud and Remote Work Challenges – As organizations migrate to cloud services and embrace remote work, attackers exploit misconfigurations, weak endpoint security, and the lack of visibility in hybrid environments.

- Zero trust ensures that access to cloud services is based on continuous validation of user identity, device posture, and location. This helps prevent attackers from exploiting misconfigured cloud resources or compromising sensitive data.

Appendix 2 – Zero Trust Case Studies

Case Study 1 – Akamai Technologies: Eliminating VPNs with Zero Trust

Industry: Content Delivery and Cloud Services.

Overview: Akamai transitioned from traditional VPN-based access to a zero trust security model, aiming to improve security and user experience.

Implementation: By adopting a zero trust framework, Akamai eliminated the need for VPNs, instead granting access based on user identity, device health, and contextual factors.

Outcomes:

- **Enhanced Security**: Reduced attack surface by verifying every access request.
- **Improved User Experience**: Provided seamless access without VPN-related latency.
- **Operational Efficiency**: Simplified access management and reduced overhead.

Lessons Learned:

- **User-Centric Approach**: Focusing on user experience can drive successful adoption.
- **Continuous Monitoring**: Ongoing assessment of device health and user behavior is crucial.

Source: How Akamai Implemented a Zero Trust Security Model Without a VPN [66]

Case Study 2 – EvolutionIQ: Cloud-Native Security with Zero Trust

Industry: Insurance Technology.

Overview: EvolutionIQ, a cloud-native startup, integrated zero trust principles to secure its predictive analytics platform for the insurance industry.

Implementation: The company adopted Google's BeyondCorp framework, emphasizing device and user authentication, and utilized cloud-native security services.

Outcomes:

- **Scalable Security**: Aligned security measures with rapid business growth.
- **Regulatory Compliance**: Met stringent industry standards for data protection.
- **Resilience**: Maintained robust security across a distributed workforce.

Lessons Learned:

- **Cloud Integration**: Leveraging cloud-native security services can streamline zero trust adoption.
- **Cultural Alignment**: Embedding security into the organizational culture enhances effectiveness.

Source: Case Study: Cloud-Native Security Using Zero Trust [67]

[66] *How Akamai Implemented a Zero Trust Security Model -Without a VPN: Akamai Case Study AKAMAI CASE STUDY*. (n.d.). https://www.akamai.com/site/en/documents/case-study/how-akamai-implemented-a-zero-trust-security-model-without-a-vpn.pdf

[67] *Case Study: Cloud-Native Security Using Zero Trust*. (n.d.). ISACA. https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/case-study-cloud-native-security-using-zero-trust

Case Study 3 – Cimpress: Enterprise-Wide Zero Trust Architecture

Industry: Mass Customization and Printing.

Overview: Cimpress, a global company specializing in customizable print products, implemented a zero trust architecture to support its complex, distributed operations.

Implementation: The organization designed a zero trust framework tailored to its multi-level maturity and diverse operational needs, focusing on identity verification and access controls.

Outcomes:

- **Unified Security Posture**: Standardized security across various business units.
- **Improved Compliance**: Ensured adherence to industry regulations and standards.
- **Operational Agility**: Enabled secure access for a dynamic, global workforce.

Lessons Learned:

- **Customization**: Adapting zero trust principles to specific organizational contexts is essential.
- **Stakeholder Engagement**: Involving all business units fosters cohesive implementation.

Source: Case Study: Building a Zero Trust Architecture to Support an Enterprise [68]

Case Study 4 – Microsoft: Internal Adoption of Zero Trust

Industry: Technology.

Overview: Microsoft transitioned to a zero trust security model to enhance protection across its global operations.

Implementation: The company focused on strong user identity verification, device health validation, and the least privilege access principles.

- **Enhanced Security**: Reduced risk of breaches through continuous verification.
- **Seamless User Experience**: Maintained productivity with minimal friction.
- **Scalability**: Applied zero trust principles across diverse services and platforms.
- **Phased Implementation:** Gradual adoption allows for adjustment and optimization.
- **Comprehensive Training:** Educating employees is critical for successful adoption.

Source: Implementing a Zero Trust security model at Microsoft [69]

[68] Teitler, K. (2021, February 26). *Case Study: Building a Zero Trust Architecture to Support an Enterprise*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/building-a-zero-trust-architecture-to-support-an-enterprise

[69] Inside Track Staff. (2023, January 11). *Implementing a Zero Trust security model at Microsoft*. Inside Track Blog. https://www.microsoft.com/insidetrack/blog/implementing-a-zero-trust-security-model-at-microsoft/

Appendix 3 – Zero Trust Misconceptions

Zero Trust Means No Trust at All

Zero trust does not imply a lack of trust in users, devices, or networks. Instead, it emphasizes earned trust that is continuously verified. Every access request is evaluated based on the user's identity, device posture, location, and behavior, ensuring that trust is neither implicit nor permanent.

Zero Trust a Single Product or Technology

Zero trust is not a one-size-fits-all product or a specific technology. Zero trust is a security strategy that combines tools, processes, and policies to enforce the least privilege access and continuous verification. While tools like MFA, micro-segmentation, and IAM are part of zero trust, no single product can ever offer a complete zero trust solution.

Zero Trust Is Only About Network Security

Although network segmentation and secure access are core components, zero trust extends beyond network security. Zero trust encompasses identity verification, application security, data protection, and device compliance. The goal is to protect all assets, whether on premises, in the cloud, or across hybrid environments.

Zero Trust Is Only for Large Organizations

While large enterprises are early adopters, zero trust is equally relevant for Small and Medium-Sized Businesses (SMBs). Cyber threats do not discriminate based on size, and zero trust principles (like verifying every access request and reducing attack surfaces) which are scalable to organizations of all sizes.

Zero Trust Is Too Expensive for Small Businesses

Zero trust, often associated with large enterprises, is not inherently cost-prohibitive and can be adopted incrementally by small businesses. By leveraging existing tools, implementing low-cost or open-source solutions, and prioritizing critical assets, small organizations can focus on affordable, high-impact measures. As a scalable framework, zero trust allows businesses to start with manageable steps, such as enforcing least privilege access or endpoint protection, laying the foundation for advanced capabilities as resources grow; all while enhancing security without overextending budgets.

Zero Trust Eliminates All Cyber Risks

Zero trust significantly reduces the attack surface and improves an organization's ability to detect and respond to threats, but it does not guarantee total immunity from cyberattacks. Instead, zero trust focuses on minimizing risks and ensuring that breaches are contained and do not propagate across systems.

Zero Trust Implementation Is a One-Time Project

Zero trust is a continuous journey, not a single implementation effort nor a project. As technology evolves and new threats emerge, organizations must regularly update their zero trust strategies, policies, and technologies to remain effective.

Zero Trust Creates Friction for Users

When designed well, zero trust can enhance user experience by reducing unnecessary access permissions and streamlining authentication through adaptive access controls. By leveraging automation and intelligent policies, organizations can strike a balance between security and usability.

Zero Trust Requires Replacing All Existing Infrastructure

Zero trust does not necessitate a complete overhaul of existing systems. Instead, it can often integrate with current tools and technologies, allowing organizations to gradually adopt zero trust principles. Many existing security solutions can be reconfigured to align with zero trust objectives.

Appendix 4 – Glossary of Terms

Attack Surface: The set of points on the boundary of a system, a system component, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, component, or environment.[70]

Note: In zero trust, an attack surface is referred to a protect surface, representing the difference in thinking and approach when adopting and aligning with zero trust.

Capability:

- A [device] feature of function; a person's potential to accomplish something.
- A combination of mutually reinforcing security and/or privacy controls implemented by technical means, physical means, and procedural means. Such controls are typically selected to achieve a common information security- or privacy-related purpose.[71]

Cloud Infrastructure Entitlement Management (CIEM): capabilities facilitate the management of identities and entitlements in cloud and multi-cloud environments.

Cloud-Native Application Protection Platform (CNAPP): capabilities help align the visibility and security protections for deployed cloud applications

Cloud Security Posture Management (CSPM): capabilities facilitate monitoring in cloud and multi-cloud environments by identifying, alerting on, and mitigating cloud vulnerabilities. Some CSPM capabilities that focus on managing and securing SaaS applications may be referred to as SaaS Security Posture Management (SSPM) solutions.

Cloud Workload Protection Platforms (CWPP): can help facilitate visibility and management of security controls in cloud and multi-cloud environments, commonly including functions like system hardening, vulnerability management, host-based segmentation, system integrity monitoring, and application allow lists.

IT governance is a set of formalized standards and processes that businesses follow to ensure that all IT investments are necessary, feasible, and deliver bottom-line results. IT governance frameworks are designed so organizations can reduce the likeliness of risks and losses due to unethical or improper management of data, technology, and business operations.

Microsegmentation is a security design practice where an internal network (e.g., in the data center, cloud provider region) is divided into each segment that can be monitored and controlled. The primary purpose of microsegmentation is to provide a degree of isolation to prevent attack escalation.[72]

Protect Surface entails identifying, categorizing, and assessing an organization's Data, Applications, Assets, and Services (DAAS); business risk; and current security maturity.[73]

[70] Editor, C. C. (n.d.). *attack surface - Glossary | CSRC*. Csrc.nist.gov. https://csrc.nist.gov/glossary/term/attack_surface

[71] CSRC Content Editor. (2025). *capability - Glossary | CSRC*. Nist.gov. https://csrc.nist.gov/glossary/term/capability

[72] Chandramouli, R. (2022). Guide to Secure Enterprise Network Landscape. *Guide to a Secure Enterprise Network Landscape*. https://doi.org/10.6028/nist.sp.800-215

[73] *Defining the Zero Trust Protect Surface | CSA*. (2024). Cloudsecurityalliance.org. https://cloudsecurityalliance.org/artifacts/defining-the-zero-trust-protect-surface

Resource: Devices, files, records, tables, directories, databases, mini-disks, processes, programs, domains. current security maturity; [an] asset used or consumed during the execution of a process.[74]

Security Information and Event Management (SIEM): A program that provides centralized logging capabilities for a variety of log types.[75]

SIEM supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other events and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting).[76]

Security Orchestration, Automation and Response (SOAR): refers to technologies that enable organizations to collect inputs monitored by the security operations team. For example, alerts from the SIEM system and other security technologies (where incident analysis and triage can be performed by leveraging a combination of human and machine power) help define, prioritize, and drive standardized incident response activities. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format. Gartner.[77]

WAF is a firewall class that has been used ever since web applications accessed through web protocols, such as Hypertext Transfer Protocol (HTTP), came into existence. A feature advancement in this class of firewalls is advanced Uniform Resource Locator (URL) filtering. This is the ability to detect traffic from malicious URLs and prevent web-based threats and attacks by receiving real-time data analyzed by machine learning algorithms. Specifically, this class of firewalls can inspect threat vectors for SQL Injection, Operating System (OS) command injections, and cross-site scripting attacks, as well as prevent inbound attacks. They are used in Content Delivery Networks (CDN) and to prevent Distributed Denial-Of-Service (DDoS) attacks. Some additional features found in this class of firewalls are:[78]

- Ability to specify an allowable list of services (control at the application level).
- Traffic matches the intent of allowed ports.
- Filtering of some unwanted protocols.

ZTA is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.[79]

[74] Ross, R., Winstead, M., McEvilley, M., Computer Security Division, The MITRE Corporation, U.S. Department of Commerce, & National Institute of Standards and Technology. (2022). *Engineering trustworthy secure systems*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf

[75] Johnson, A., Dempsey, K., Ross, R., Gupta, S., Bailey, D., Computer Security Division, Information Technology Laboratory, & Electrosoft Services, Inc. (2011). Guide for Security-Focused Configuration Management of Information Systems. In *NIST Special Publication 800-128* [Report]. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf

[76] Gartner. (2019). *Security Information And Event Management (siem)*. Gartner. https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

[77] *Definition of Security Orchestration, Automation and Response (SOAR) - Gartner Information Technology Glossary*. (n.d.). Gartner. https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar

[78] Chandramouli, R., National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, & U.S. Department of Commerce. (2022). Guide to a secure enterprise network landscape. In *NIST Special Publication (SP) 800-215*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-215.ipd.pdf

[79] Rose, S., Borchert, O., Mitchell, S., Connelly, S., National Institute of Standards and Technology, Advanced Network Technologies Division, Stu2Labs, & Cybersecurity & Infrastructure Security Agency. (2020). *Zero trust architecture*. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

Appendix 5 – Reference Sources

The following were referenced in the creation of this document.

1. Washington State Statute – Office of cybersecurity – State CISO – State Agency Information Technology Security
   a. URL ref: (https://app.leg.wa.gov/rcw/default.aspx?cite=43.105&full=true#43.105.450)
2. WaTech's Security Service Edge (SSE) Onboarding Project
   a. URL ref: (https://watech.wa.gov/security-service-edge-sse-onboarding-project)
3. National Association of State Chief Information Officers – State CIO Top Ten Policy and Technology Priorities for 2025
   a. URL ref: (https://www.nascio.org/resource-center/resources/state-cio-top-ten-policy-and-technology-priorities-for-2025/)
4. Washington State Enterprise IT Strategic Plan
   a. URL ref: (https://watech.wa.gov/strategy/enterprise-it-strategic-plan)
5. Washington State Executive Order 24-01 – Artificial Intelligence
   a. URL ref: (https://governor.wa.gov/sites/default/files/exe_order/24-01%20-%20Artificial%20Intelligence%20%28tmp%29.pdf)
6. National Institute of Standards and Technology – Zero Trust Architecture
   a. URL ref: (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf)
7. Washington State Cloud Smart Strategy
   a. URL ref: (https://watech.wa.gov/sites/default/files/2023-11/State%20of%20Washington%20Cloud%20Strategy%201.0%20Published.pdf)
8. Washington State Statute – Broadband office
   a. URL ref: (https://app.leg.wa.gov/rcw/default.aspx?cite=43.105&full=true#43.105.450)
9. Gartner Implement Zero-Trust Architecture to Adapt to a Shifting Threat Landscape
   a. URL ref: (https://www.gartner.com/en/cybersecurity/topics/zero-trust-architecture)
10. National Institute of Standards and Technology – Cybersecurity Framework
    a. URL ref: (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf)
11. National Institute of Standards and Technology – Risk Management Framework (RMF)
    a. URL ref: (https://csrc.nist.gov/projects/risk-management/about-rmf)
12. National Institute of Standards and Technology – Security and Privacy Controls for Information Systems and Organizations
    a. URL ref: (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf)
13. Center of Internet Security – The 18 CIS Critical Security Controls
    a. URL ref: (https://www.cisecurity.org/controls/cis-controls-list)
14. Cybersecurity and Infrastructure Security Agency (CISA) – Zero Trust Maturity Model version 2.0
    a. URL ref: (https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdfhttps://www.cisa.gov/zero-trust-maturity-model)
15. Gartner Information Technology Glossary – Secure Access Service Edge
    a. URL ref: (https://www.gartner.com/en/information-technology/glossary/secure-access-service-edge-sase)
16. Cloud Security Alliance (CSA) – Cloud Controls Matrix
    a. URL ref: (https://cloudsecurityalliance.org/research/cloud-controls-matrix)
17. VMware - Incorporating VMware Zero-Trust for the Presidential Executive Order
    a. URL ref: (https://blogs.vmware.com/euc/2021/10/incorporating-vmware-zero-trust-for-the-presidential-executive-order.html)
18. Gartner – Implementing Zero Trust Security in the Public Sector
    a. URL ref: (https://www.gartner.com/en/industries/government-public-sector/topics/zero-trust)
19. Department of Defense Zero Trust Strategy
    a. URL ref: (https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf)
20. Compact – Zero Trust: beyond the hype – Published: July 2022
    a. URL ref: (https://www.compact.nl/en/articles/zero-trust-beyond-the-hype/)
21. Compact Magazine – Outdated "castle-moat" cyber defense setup [image]
    a. URL ref: (https://www.compact.nl/articles/zero-trust-beyond-the-hype/)
22. Cybersecurity and Infrastructure Security Agency – Secure by Design
    a. URL ref: (https://www.cisa.gov/securebydesign)
23. Info-Tech – Build a Zero Trust Roadmap
    a. URL ref: (https://www.infotech.com/research/ss/build-a-zero-trust-roadmap)
24. John Kindervag – Define a Protect Surface to Massively Reduce Your Attack Surface
    a. URL ref: (https://www.paloaltonetworks.com/blog/2018/09/define-protect-surface-massively-reduce-attack-surface/)
25. Department of Defense – Zero Trust Overlays

    a. URL ref: (https://dodcio.defense.gov/Portals/0/Documents/Library/ZeroTrustOverlays.pdf?)

26. Cloud Security Alliance – Defining the Zero Trust Protect Surface
    a. URL ref: (https://cloudsecurityalliance.org/artifacts/defining-the-zero-trust-protect-surface)
27. Center of Internet Security – Vulnerability Assessments
    a. URL ref: (https://www.cisecurity.org/services/vulnerability-assessments)
28. PCI Security Standards Council – PCI Data Security Standard
    a. URL ref: (https://www.pcisecuritystandards.org/standards/pci-dss/)
29. United States Department of Health & Human Services – Summary Of the HIPPA Privacy Rule
    a. URL ref: (https://www.hhs.gov/sites/default/files/privacysummary.pdf)
30. IRS - Tax Information Security Guidelines (Publication 1075)
    a. URL ref: (https://www.irs.gov/pub/irs-pdf/p1075.pdf)
31. National Institute of Standards and Technology Glossary – Personally Identifiable Information
    a. URL ref: (https://csrc.nist.gov/glossary/term/personally_identifiable_information)
32. National Institute of Standards and Technology Glossary – Intellectual Property
    a. URL ref: (https://csrc.nist.gov/glossary/term/intellectual_property)
33. Washington State Standard – Data Classification Guidance
    a. URL ref: (https://watech.wa.gov/categorizing-data-state-agency)
34. Washington State Data Classification Standard
    a. URL ref: (https://watech.wa.gov/sites/default/files/2024-09/SEC-08-01-S%20Data%20Classification%20Standard.pdf)
35. Roman Data Defense – The Threat is real
    a. URL ref: (https://romandata.com/)
36. National Institute of Standards and Technology – Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events
    a. URL ref: (https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html)
37. National Institute of Standards and Technology – Engineering Trustworthy Secure Systems
    a. URL ref: (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf)
38. SSL.com - Zero Trust Architecture: A Brief Introduction
    a. URL ref: (https://www.ssl.com/blogs/zero-trust-architecture-a-brief-introduction/)
39. Gartner Information Technology Glossary – Zero Trust Network Access (ZTNA)
    a. URL ref: (https://www.gartner.com/en/information-technology/glossary/zero-trust-network-access-ztna-)
40. Akamai - How Akamai Implemented a Zero Trust Security Model – Without a VPN
    a. URL ref: (https://www.akamai.com/site/en/documents/customer-story/how-akamai-implemented-a-zero-trust-security-model-without-a-vpn.pdf)
41. ISACA - Case Study: Cloud-Native Security Using Zero Trust
    a. URL ref: (https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/case-study-cloud-native-security-using-zero-trust)
42. ISACA - Case Study: Building a Zero Trust Architecture to Support an Enterprise
    a. URL ref: (https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/building-a-zero-trust-architecture-to-support-an-enterprise)
43. Microsoft - Implementing a Zero Trust security model at Microsoft
    a. URL ref: (https://www.microsoft.com/insidetrack/blog/implementing-a-zero-trust-security-model-at-microsoft/)
44. National Institute of Standards and Technology Glossary – Attack Surface
    a. URL ref: (https://csrc.nist.gov/glossary/term/attack_surface)
45. National Institute of Standards and Technology Glossary – Capability
    a. URL ref: (https://csrc.nist.gov/glossary/term/capability)
46. National Institute of Standards and Technology – Guide to a Secure Enterprise Network Landscape
    a. URL ref: (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-215.pdf)
47. Cloud Security Alliance – Defining the Zero Trust Protect Surface
    a. URL ref: (https://cloudsecurityalliance.org/artifacts/defining-the-zero-trust-protect-surface)
48. National Institute of Standards and Technology Glossary – Resource
    a. URL ref: (https://csrc.nist.gov/glossary/term/resource)
49. National Institute of Standards and Technology Glossary – SOAR
    a. URL ref: (https://csrc.nist.gov/glossary/term/soar)
50. Gartner Information Technology Glossary – Security Information And Event Management (SIEM)
    a. URL ref: (https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem)
51. Gartner Information Technology Glossary – Security Orchestration, Automation and Response (SOAR)
    a. URL ref: (https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar)
52. National Institute of Standards and Technology Glossary – Zero Trust Architecture
    a. URL ref: (https://csrc.nist.gov/glossary/term/zero_trust_architecture)

Manuscript Contact

Questions and comments regarding this white paper can be directed to:

Mikel B. Costello
Strategic Planning and Design Manager
Washington Technology Solutions (WaTech)
Mike.costello@watech.wa.gov