COMPUTER WORLD SERVICES

Zero Trust Digital Transformation

CWS

VISION

Premiere Provider of Digital Transformation and Cybersecurity Services to the Federal Government

Executive Summary

In response to the evolving threat vectors exploited by foreign and domestic “Bad Actors”, Zero Trust has emerged as the paradigm shift that modernizes legacy-based perimeter security to a granular entity, permissions, roles and activity access controls designed to protect data, systems, and infrastructure. Zero trust assumes there is no implicit trust granted to users, systems, services and applications based solely on their core General Support System access. With Zero Trust, system access MUST be authenticated and authorized before a session to an enterprise system or resource is established. Fundamentally, Zero Trust protects users, systems, infrastructure and the enterprise from direct attacks, lateral attacks, unauthorized access and data exposure by restructuring layered security archetype. The hidden “gem” in Zero Trust is that it is not a product, technology stack or infrastructure an organization needs to purchase. Instead, it is a Cybersecurity strategy that incorporates precise rules and risk-based policies, coupled with micro-segmentation and strong identity management to protect ALL digital assets.

Federal Imperative

The significance of Zero Trust has been highlighted by the Office of Management and Budget (OMB) on January 26, 2022 Memorandum, M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. In support of Memorandum M-22-09, National Institute of Standards and Technology (NIST) released NIST Special Publication 800-207, Zero Trust Architecture. As one of the leading information technology services providers for the federal government, Computer World Services is poised and ready to assist you in complying with the federal mandate and helping ensure your agency maintains a positive and resilient cybersecurity profile. We have the people, experience, and solutions to support you through every step of your Zero Trust journey. Our Corporate experience with Zero Trust Architecture (ZTA) will assist the development and execution of an agency’s enterprise cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies.

Zero Trust Framework

Seven Tenets of Zero Trust

The Seven Tenants of Zero Trust is an integrated strategy for always authenticating and verifying all users, devices, and systems. Taken literally, Zero Trust means no trusted devices or users will be able to access assets without verification. Any attempted activity without authorization will not be allowed and reported. The Seven Tenants of Zero Trust lays a comprehensive foundation for implementing and executing the new security controls under the ZTA paradigm.

1. **All data sources and computing services are considered resources.**
   - Everything on the corporate network is the agency's responsibility. Effective Zero Trust encompasses every device and service that may be accessed by the corporate network
2. **All communication is secured regardless of network location.**
   - All data in transit must be encrypted. Preserve the confidentiality and integrity of all corporate communications with encryption
3. **Access to individual enterprise resources is granted on a per-network session basis.**
   - Validate user access, roles and rights for every enterprise asset. No more "Blanket access" to enterprise asset(s) once logged into the network.
4. **Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.**
   - Design, implement and enforce comprehensive asset access policies for users and system accounts. Leverage technology and processes that have the capability to continuously authenticate attributes, artifacts, behavior and patterns.
5. **The enterprise monitors and measures the integrity and security posture of all owned and associated assets.**
   - Continually monitor the security posture of all of the enterprise devices to ensure they are compliant and enforce the zero trust access policies and technical security specifications (Updated, patched and monitored)
6. **All resource authentication and authorization are dynamic and strictly enforced before access is allowed.**
   - The Identity, Credential, and Access Management (ICAM) and asset management systems integration coupled with multifactor authentication (MFA) for access essential for Zero Trust enables controlled access
7. **The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.**
   - Log, capture and assess ALL enterprise activity leveraging a continuous diagnostics and mitigation (CDM) strategy. Real time enterprise activity visibility is a core capability and part of the triage and forensic restoration loop

To Zero Trust, "**Everything is a Resource**"

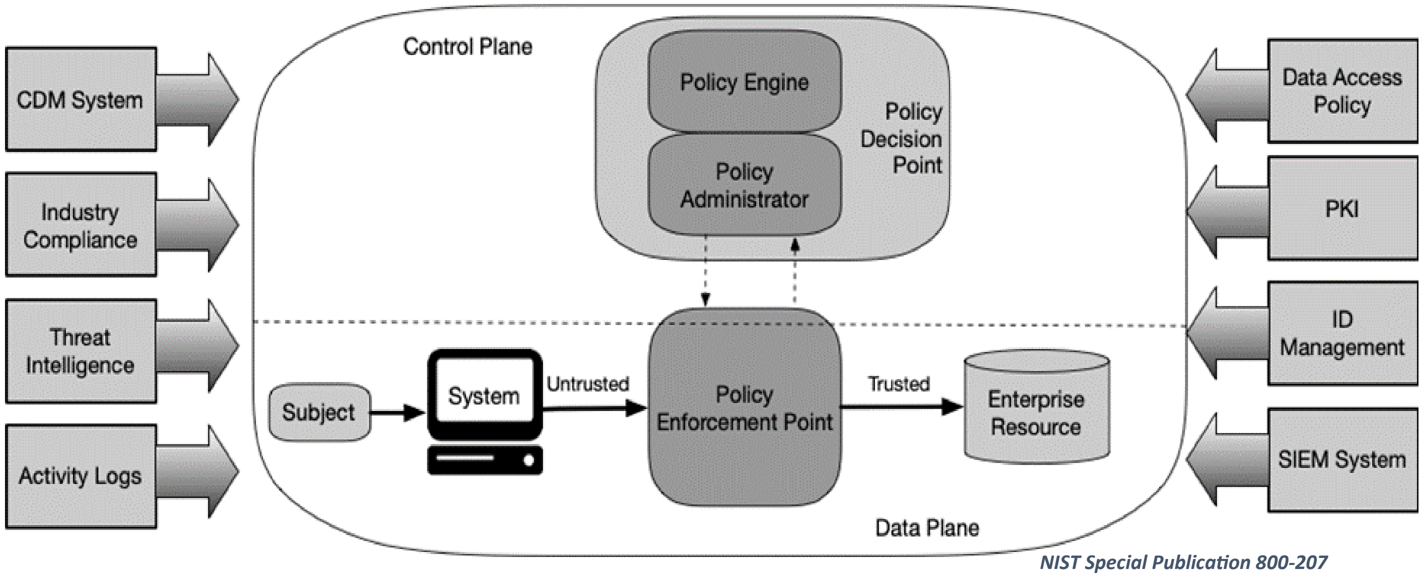
Grant the lowest level of access. Ensure open sessions are closed ASAP. Eliminate blanket authorizations. Monitor, Track & Manage network traffic and system activity.

COMPUTER WORLD SERVICES

Zero Trust Architecture

Foundation of Zero Trust

While the concepts of Zero Trust are straightforward, the implementation of Zero Trust Architecture (ZTA) in your environment can be complex. Shifting the security perimeter from a layer/boundary paradigm to ZTA's entity-based authentication and authorization approach can be a challenge. Restructuring your identity management system(s) and tools coupled with developing granular user access policies and workflows is a substantial task. A very good depiction of the new model is articulated in NIST Special Publication 800-207, the Logical Components of Zero Trust Architecture is at the center of a Zero Trust solution.



NIST Special Publication 800-207

GOVERNANCE STANDARD

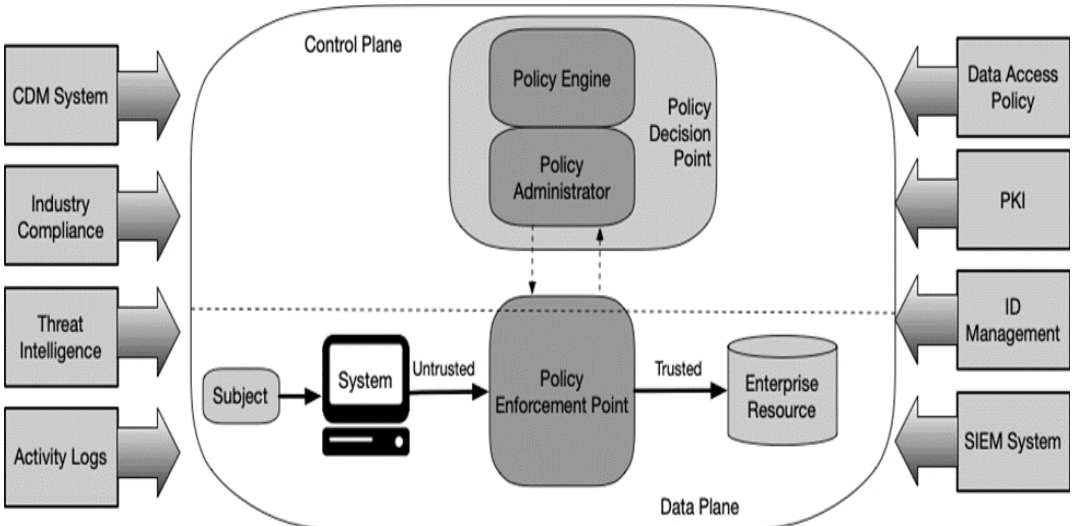
NIST's SP 800-207 is a major paradigm shift for cybersecurity. The new Zero Trust Architecture restructures and focuses security on effective and secure management of identities, authentication, and authorization. It obfuscates the perimeter and eliminates implicit enterprise trust. The new verify, control and allow model for users, assets and resources provides enhanced capabilities and superior granular controls that strengthen the security posture for an enterprise.

Logical Components of Zero Trust Architecture

Logical Components Defined

Policy Engine The Policy Engine (PE) is responsible for the ultimate decision to grant access to a resource. The PE is paired with the Policy administrator component. The policy engine makes and logs the decision (as approved, or denied), and the policy administrator executes the decision.

Policy Administrator This component is responsible for establishing and/or shutting down the communication path between a subject and a resource (via commands to relevant PEPs). The PA authenticates and dynamically authorizes all access requests based on policy decisions by the PE. The authorization is based on context attributes, trust levels and security strategies



NIST Special Publication 800-207

Policy Enforcement Point (PEP) The PEP is the core component to implement the capability of continuous trust evaluation in a Zero Trust architecture. The PEP combines behavioral analytics, external threat intelligence, enterprise security policy, regulatory requirements and identity and authority baselines to evaluate and generate access decisions (grant, deny or revoke access).

Continuous diagnostics and mitigation (CDM) This component provides the required visibility into the status of the corporate resources, and applies updates to configuration and software components. CDM systems are also responsible for identifying and potentially enforcing a subset of policies on privately-owned devices operating within the enterprise infrastructure, enhancing trust.

Industry compliance Ensures the compliance of corporate policies with regulatory security requirements. Such regulations from FISAM, NIST, DoD and the healthcare and others as applicable.

Logical Components of Zero Trust Architecture

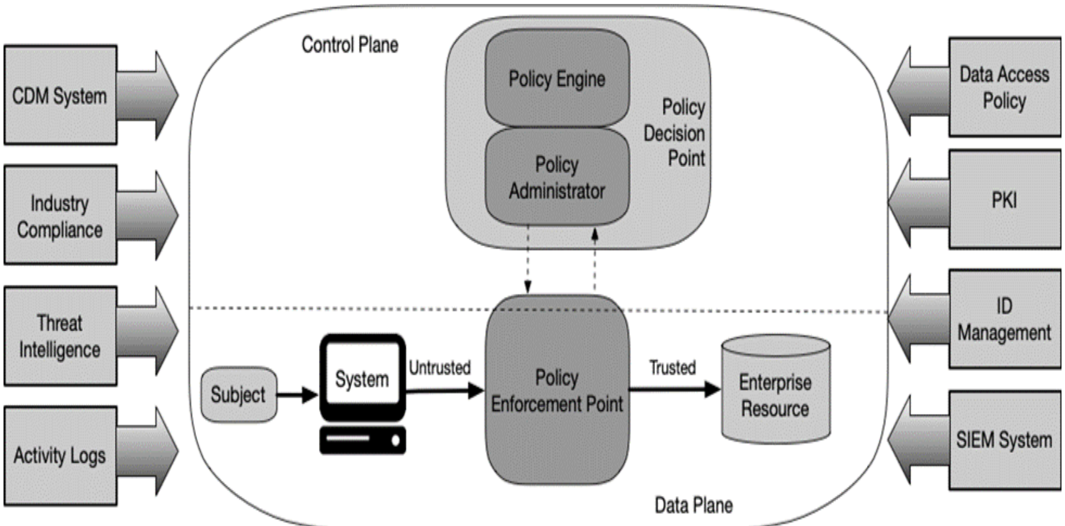
Logical Components Defined

Industry compliance Ensures the compliance of corporate policies with regulatory security requirements. Such regulations from FISMA, NIST, DoD, healthcare and others as applicable.

Threat intelligence Provides information from internal or external sources about newly discovered attacks or vulnerabilities that help make dynamic and adaptive access determinations.

Network and system activity logs Aggregates asset logs, network traffic, resource access actions, and other events that provide real-time (or near-real-time) feedback on the security posture of enterprise information systems.

Data access policies These define the attributes, rules, and policies about access to enterprise resources. These policies form the foundation for authorizing access to a resource as they provide the basic access privileges for accounts and applications/services in the enterprise.



NIST Special Publication 800-207

Enterprise public key infrastructure (PKI) This system is responsible for managing the lifecycle of digital certificates (X.509) issued by the enterprise to resources, subjects, services and applications.

Identity management system This is responsible for creating, storing, and managing both enterprise user accounts and identity records and federated non-enterprise, partner accounts. This system contains the necessary subject information (e.g., name, email address, certificates) and other enterprise characteristics such as role, access attributes, and assigned assets.

Security information and event management (SIEM) This collects security-centric information for later analysis to refine policies and warn of possible attacks against enterprise assets.

Demonstration of Expertise

Project NEO

Computer World Services Corp was extended the opportunity to implement some of the Zero Trust methodologies for DISA. CWSC was asked to modernize an unautomated process which was managed by multiple organizations within and outside of DISA, with legacy communications between systems, with unneeded processes, numerous personnel, and disparate security silos. Our experience and collaboration with process and system engineers significantly streamlined the overall process and created a Zero Trust Network environment.

Code named project NEO. Project NEO was the full automation of DISA's onboarding process for new and leaving users. The project focused on integrating their new ticketing system ServiceNow into SailPoint and developing automated account provisioning with ServiceNow being the source of authority and all intermediary points moving to zero trust.

The CONOP for Project NEO is to facilitate the process of a new DISA user onboarding through a ServiceNow portal, SailPoint aggregates those onboarding ticket attributes and then it communicates out to build the user DISA user's identity. This includes the users email account and permissions, Active Directory profile and permissions, all share drive accesses, and more. The Out-processing process function is similar but in reverse synchronization steps. This significantly reduced administrative overhead and increased security and efficiency.

Quality & Confidence

Computer World Service's Best Product

Quality & Confidence are the best product and services CWS provide. Our commitment to excellence and to our customers is unmatched. We consistently bring the best people, strategy, resources and professionalism to every customer. We are the "Home Run" your Agency deserves.

Real World Zero Trust

PRIORITIES

Mission

People

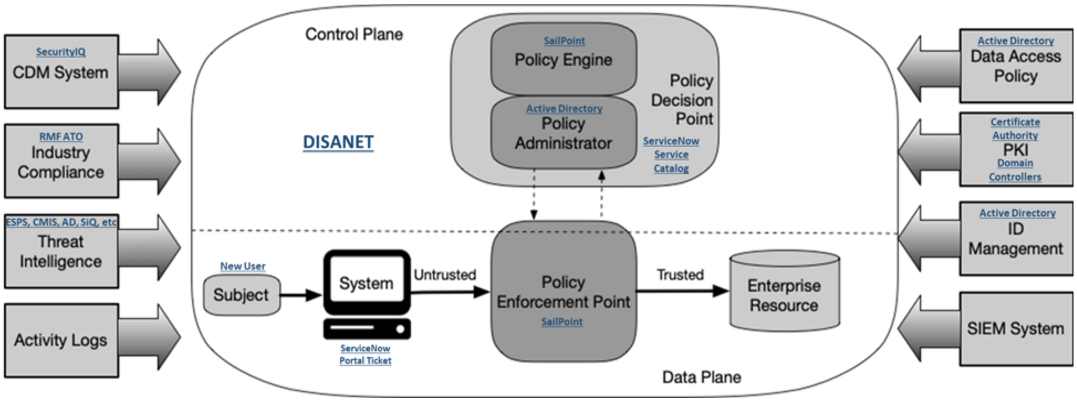
Quality

Customers

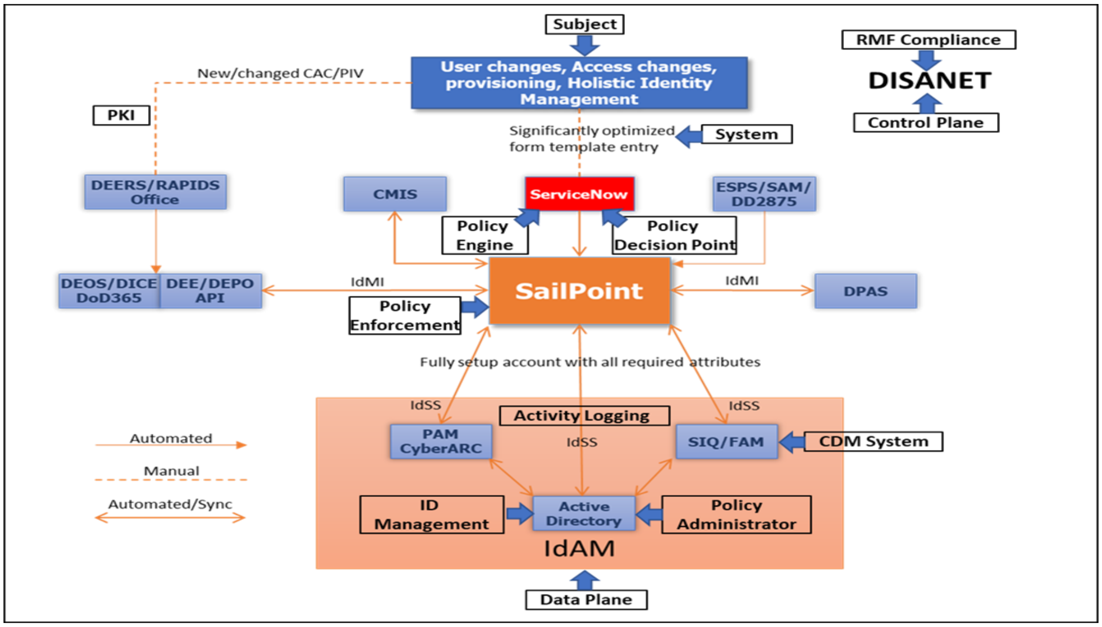
Fulfillment

Project Neo

CWS utilized sophisticated Zero Trust IAM/IDM techniques and leveraged the NIST Zero Trust Architecture Framework to implement an effective, secure and compliant solution to integrate SailPoint with zero trust synchronization with ServiceNow and Active Directory for our DISA customer.



Through CWS's comprehensive understanding and mastery of Zero Trust concepts, processes and IT technologies, we integrated DISA's existing infrastructure with the NIST 800-207 Zero Trust Architecture guidance to deliver and fully functional the Zero Trust based Onboarding and Offboarding provisioning system for our DISA Customer.



Customer Experience

Project NEO, Before and After

Project NEO is a success story. Team CWS was able in to introduce efficiencies, enable additional capacity, increase quality, streamline processes, increase visibility, and increase security. All by implementing Zero Trust Architecture with DISA's existing infrastructure. We preserved and added additional value to their current investment.

Element	Legacy Design	CWS' ZTA Solution
Number of people involved in process	100+	7
Number of days to accomplish process	14+	1
Number of depts to accomplish process	7+	2-3
Time required to complete the process	40+	8
Manual Processes in Overall system	11	2

LEGACY DESIGN

- Highly manual process with multiple system integration points, a significate number of attributes to synchronize
- Limited to no process visibility and task notification capabilities
- Multiple supervisor approvals requirement
- Notable error rate which caused

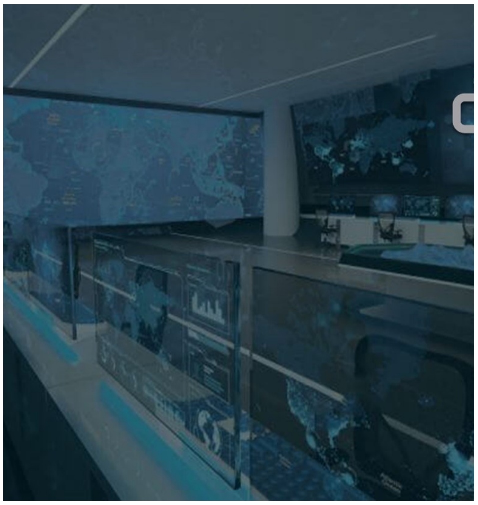
CWS ZTA SOLUTION

- Enabled API and system attribute synchronization with SailPoint and ServiceNow
- Implemented automated workflow
- Significant reduction a manual process and manual data entry
- Streamlined approvals based on automated evaluation criteria

<u>Work with CWS!</u> We can help you meet Executive Order 14028 – Improving the Nation's Cybersecurity and help you Modernize the Federal Government's Cybersecurity.

CWS

Contact Us



HEADQUARTERS

6402 Arlington Blvd
Suite 650
Falls Church, VA 22042
202.637.9699

ILLINOIS

16 Executive Drive
Suite 260
Fairview Heights, IL 62208
618.433.3006

Vehicles

CIO-SP3 Services & Solutions CIO-SP3 Small Business Services & Solutions	GSA Multiple Award Schedule (MAS)	Information Management Communications Services 3 (IMCS III)	Information Technology Enterprise Solutions 3 Services (ITES-3S)

Appraisals and Certifications

CMMISVC/3℠
CMMISVC2.0 / Exp. 2023-12-11 / Appraisal #51711

Certified System ™
ISO 9001
QMI-SAI Global

NSF
NSF-ISR
Registered to ISO/IEC 20000

NSF
NSF-ISR
Registered to ISO 27001