White paper
Cisco public

The bridge to possible

Zero Trust 101

Enabling your agency's mission

U.S. Public Sector

Evolving the Federal government's security model

Today's information technology has fundamentally transformed the way we work. Mobility and the cloud have enabled workers to access applications and data from anywhere. Data, especially from the edge, is about to further transform the way government employees solve problems and deliver services to our citizens.

This same technology has rendered traditional approaches to protecting our government systems and data insufficient. Multi-cloud, the edge, and mobility have stretched traditional perimeter-based cybersecurity beyond the breaking point. Fortunately, Zero Trust is more than the latest buzzword. It's a game changer, powered by Artificial Intelligence (AI) and Machine Learning (ML), with the potential to substantially enhance government agencies' abilities to protect their technology systems and data in a dynamic, continuous, and highly granular way.

Importance to digital transformation of Federal government

The Federal Government has launched numerous "Digital Transformation Initiatives" in order to "harness the power of data" to drive faster, more efficient decision making to further enhance mission outcomes and better serve citizens. The implementation of comprehensive data strategies, enabled by evolving AI data-science algorithms, are essential for agencies to achieve their goals and for our nation's continued global leadership in technology.

Implementing a Zero Trust Architecture that protects data, systems, and network infrastructures from growing cyber threats is an absolute necessity for any Federal digital transformation initiative. Federal CIO Suzette Kent, stresses that "**The Zero Trust framework underpins CDM, Einstein, TIC and TIC 3.0, ICAM, HVA and supports the goal of IT Modernization**." A Federal Zero Trust Architecture must be capable of automatically translating an agency's mission-focused intent into secure implementation of trust-based policies across the entire network environment, at speed and scale. The goal for the AI/ML-powered Zero Trust network is to continuously monitor, adapt, and adjust to drive secure, access-enabling mission accomplishment.

The bridge to possible

Contents

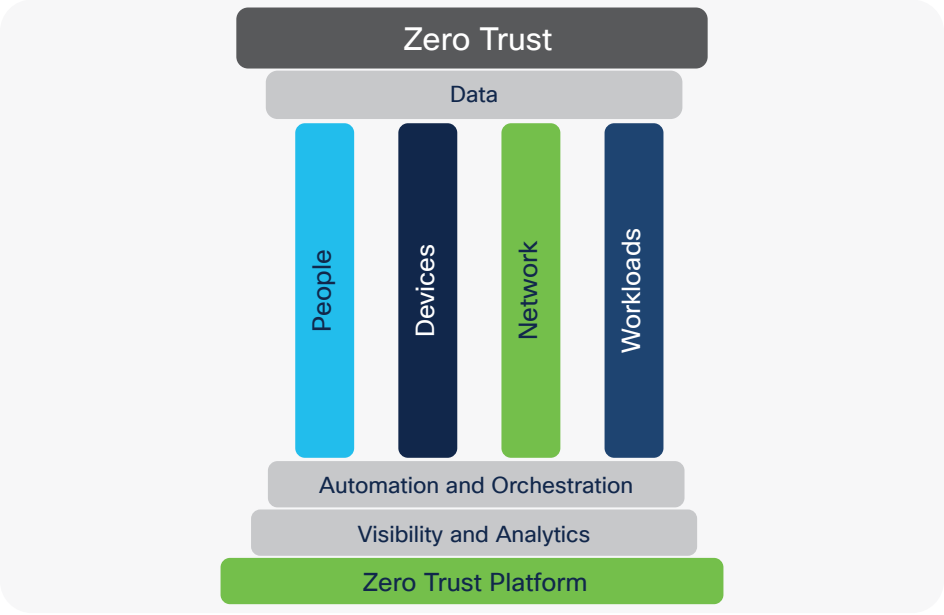
What is Zero Trust?

Zero Trust is an approach to help achieve more pragmatic security for today's world. It's a security architecture and enterprise methodology, not a technology or tool, designed to effectively orchestrate today's challenging combination of technologies, practices, and policies. It represents an evolution in our approach to security, and is focused on delivering a comprehensive, interoperable, and holistic solution approach that integrates multiple vendors' products and services.

Zero Trust Architectural Framework

A Zero Trust Architectural Framework involves restricting access to system, application, and data resources to those users and devices that are specifically validated as needing access. It will then continuously authenticate their identity and security posture to ensure proper authorization for each resource to provide continued, ongoing access.

An effective Zero Trust Architectural framework coordinates and integrates across seven main areas of focus to create an enabling platform as shown. Visibility and analytics provide the awareness for automation and orchestration, to coordinate security policies and actions across people, devices, network(s), workloads, and data.



Zero Trust background

Zero Trust is generally recognized to focus on the need to protect an organization's systems and data on multiple levels using a mixture of encryption, secure computer protocols, and dynamic workload and data-level authentication and authorization, rather than relying solely on an external network boundary.

Other Zero Trust Frameworks

Although Zero Trust is most commonly identified with Forrester (since they coined the term), many others have identified similar Zero Trust-enabling strategies and frameworks, with the most prominent being (in chronological order):

Google

BeyondCorp

A cloud-focused framework.

Gartner

Continuous Adaptive Risk and Trust Assessment (CARTA)

Includes heavier emphasis on threat than traditional Zero Trust.

John Hopkins Applied Physics Laboratory

Integrated Adaptive Cyber Defense (IACD) Focus

A commercial-off-the-shelf (COTS) tool integration approach.

NIST

Zero Trust Architecture - Draft Special Publication 800-207

An emerging architecture-focused framework.

This security concept, known as deperimeterization, is designed for a world where the traditional network perimeter is less effective as workloads are increasingly being delivered from the cloud, and mobile endpoints are becoming the norm for application and data access. Deperimeterization grew out of discussions with corporate Chief Information Security Officers (in a meeting hosted by Cisco in 2003) and was formalized in 2004 by the international Jericho Forum group.

Forrester Zero Trust

The term Zero Trust itself was created by Forrester in 2010 with the release of their **Zero Trust Network Architecture** Report. Zero Trust has become increasingly popular within the security community over the last decade. In recent years, Forrester has broadened their view of Zero Trust to cover both a **Zero Trust eXtended Ecosystem** and a **Zero Trust eXtended Ecosystem Platform**.

Today, the term Zero Trust Architecture (ZTA) is the generally accepted expression for a security environment that allows “no implicit trust.”

Critical Zero Trust Architectural considerations

Zero Trust today is really about an orchestrated approach to achieving the “de-Frankenstein-ization” of our current, dizzying approach towards security. One that stitches together dozens of security tools and products in an effort to protect an agency’s data, applications, and workloads. With an AI/ML-driven, Software Defined Network (SDN) environment, agencies can enforce privileged network access, manage data flows, contain lateral movement ,and provide visibility to make dynamic policy and trust decisions. NIST’s Zero Trust architectural approach focuses on the core logical components of a SDN strategy using a Policy Engine and Policy Administrator to form a Control Plane to restrict access to resources via Policy Enforcement Point(s) in a Data Plane.

A Zero Trust Architecture requires an open, scalable foundation to provide agencies with the means to support any relevant framework that guides their specific security needs (NIST RMF/CSF, CDM, CJIS, HIPAA, etc.). This foundational approach should be comprehensive in nature and support integrated interoperability across any security policy, governance, ICAM, SIEM, SOAR, or MDM tools in which agencies have already made investments. By tightly coupling network policy with an agency’s intent-based mission network capabilities, an AI/ML-enabled Zero Trust Architecture adds greater network context, learning, and assurance to securely accomplish its mission. Needed capabilities include:

- Granular microsegmentation of access to individual users, devices, applications, workloads, and data.
- Enforcement of security policies everywhere agency work is performed(across LANs, WANs, data centers, clouds, and the edge).

The bridge to possible

Key perspectives for agencies to embrace on their Zero Trust Journey

- Do not allow implicit trust for anyone or anything attempting to connect to key networks, systems, data, or other resources.
- Explicit authentication and authorization should be made before allowing access and then activity is continuously monitored for changes.
- Implement a software defined networking and access approach to make the network easier to configure, operate, and maintain in the face of growing scale and complexity.
- Be able to detect and effectively respond to anomalous activity in real-time at individual user, device, application, or workload levels.
- Enable comprehensive visibility, analytics, and proactive response actions across your entire communications access and security infrastructure.

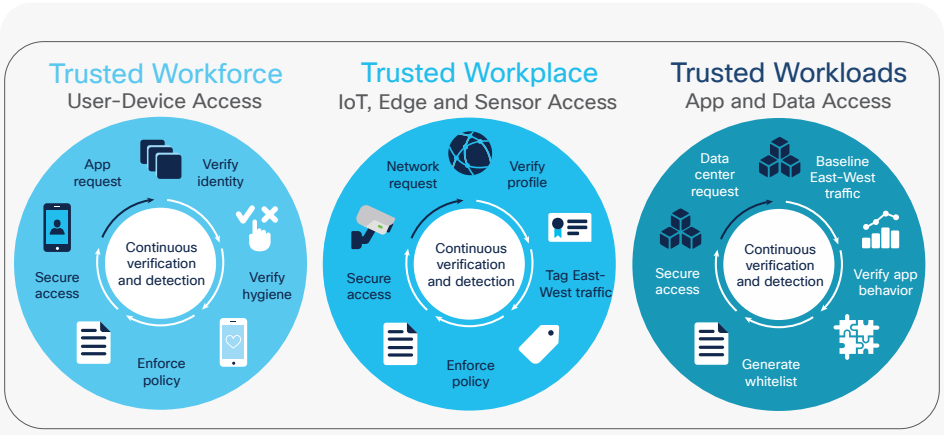
- Comprehensive identity management – extending identity and access management beyond end-users to devices and sensors/in essence, the identities of users, devices, applications, workloads, and data become new micro-perimeters via software-defined access.
- Integrated threat defense that leverages global threat intelligence and feeds.
- Automated, agile control of your agency's network to securely operate at the desired scale, performance, and reliability required for mission accomplishment.

Comprehensive Zero Trust

The key to comprehensive Zero Trust is extending security throughout the entire network environment – LAN/Campus-WAN-Data Center-Cloud-Edge -not just at the network's external perimeter. This security must include total visibility of your agency's network environment. Key elements of comprehensive Zero Trust center around:

- **Eliminating unauthorized network trust.** Assume that all traffic, regardless of location, is a potential threat until it is verified (inspected, authorized, and secured).
- **Segmenting network access.** Adopt a least-privileged strategy and strictly enforced, granular controls so users have access only to the resources needed to perform their job.
- **Gaining comprehensive visibility and analytics.** Continuously inspect and log all traffic both internally and externally, using real-time protection capabilities to monitor for and respond to malicious activity.
- **Proactively managing risk.** Acting, in real time, when anomalous activity is detected in order to minimize threat impact and optimally manage risk.

Achieving Zero Trust (aka Trusted Access)



The bridge to possible

The Current state of industry's ability to support your Zero Trust journey

To get a more detailed sense of the latest ability of industry's ability to support Zero Trust, download Forrester wave™ Zero Trust eXtended Ecosystem Platform Providers.

To achieve comprehensive Zero Trust security, Agencies must extend their Zero Trust approach across their workforce, entire workplace, and workloads.

- **Zero Trust Workforce.** Users and devices must be authenticated, authorized and access and privileges continuously monitored and governed to protect agency resources.
- **Zero Trust Workplace.** Access must be controlled across the entire workplace, including the cloud and edge. This is especially important as greater use of IoT and machine-to-machine sensors are becoming increasingly critical to successful agency mission and business outcomes.
- **Zero Trust Workloads.** Granular access control must be enforced across entire application stacks, including between containers, hypervisors, and microservices in the cloud as well as traditional agency data centers.

Cisco, a Forrester-recognized Zero Trust Leader, is a strong supporter of Zero Trust-enablement of your mission success. In addition to leveraging your Cisco networking infrastructure as a key foundation of your Zero Trust Architecture, you can learn about other key Cisco Zero Trust security capabilities that can help your agency on your Zero Trust journey. These include Identity Services Engine for granular network access control (Cisco ISE), multi-factor authentication and identity access control (Cisco Duo), malware protection control (Cisco AMP), workload protection (Cisco Tetration), cloud security (Cisco Umbrella), and anomalous activity detection and response (Cisco Stealthwatch).

Summary

One of the simplest ways to think about Zero Trust is to fine-tune the old Russian proverb, popularized by President Reagan, from "trust, but verify" into "Never Trust AND Always Verify." This applies to every connection, every session, and every request for access to critical agency applications, workloads, and data.

A Zero Trust Architectural approach, based on a logically defined, software-enabled Control Plane/Data Plane Model, ensures that every decision to access data by any user, device or workload is securely, dynamically, and continuously authenticated and authorized at the speed of AI/ML-enabled networks.

Successfully implemented, Zero Trust can help ensure secure and seamless operations across an agency's entire information technology ecosystem and result in continual trusted access to an agency's critical workloads, applications, and data—thereby enhancing your agency's missions.

C11-743532-00 04/20