The bridge to possible

Cisco Government Thought Leadership

Security resilience for government

Trend overview

On January 26, 2022, the Office of Management and Budget (OMB) issued an executive order, Order M-22-09, mandating all federal agencies to implement a Zero Trust Architecture (ZTA). The executive order requires government agencies to follow the guidelines set by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 to take an enterprise-wide architecture and isolation strategy with the goal of preventing unauthorized access to data and services coupled with making the access control enforcement as granular as possible. Each U.S. federal agency, in consultation with DHS CISA, must develop a ZTA roadmap that describes how the agency intends to isolate its applications and environments.

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Model includes a maturity model of capabilities across five distinct pillars—including Identity, Device, Network/ Environment, Application Workload, and Data. These pillars are supported across three foundational capabilities: Visibility and Analytics, Automation and Orchestration, and Governance. CISA's maturity model underscores that there are many paths to support the transition to zero trust.

The Department of Defense Zero Trust Reference Architecture, Version 2.0, published in June 2022, captures how the DoD continues to mature and develop capabilities that can be used to advance enterprises operating on the DoD Information Network (DODIN). Like the CISA model, the DoD's reference architecture defines seven similar pillars and expands each with technology-focused capabilities under each pillar. Visibility & Analytics and Automation & Orchestration are defined as separate "pillars" vs. "foundational" capabilities found in the CISA model.

Cited by both the DHS CISA and DoD models, NIST SP 800-207 identifies that zero trust "is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated." Additionally, NIST identifies that a ZTA is "an end-to-end approach to enterprise resource and data security that encompasses identity (person and non-person entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure."

Like the CISA and DoD models, NIST also recognizes that implementing zero trust is not a single solution, but a "journey" that must be undertaken in conjunction with an organization's risk managed approach.

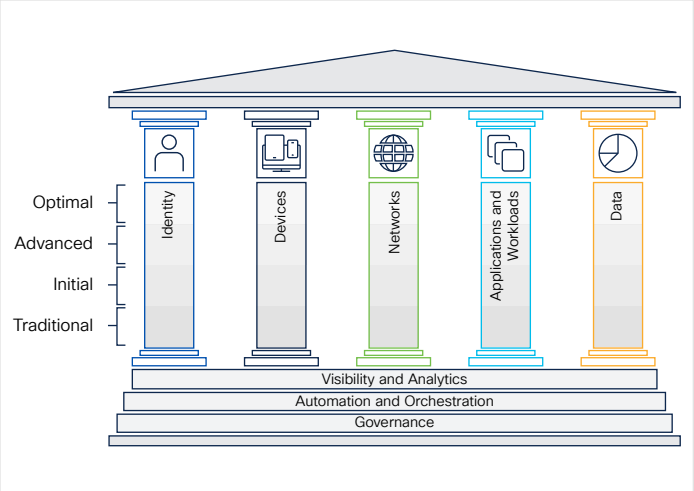

Figure 1. CISA Zero Trust Maturity Model

The bridge to possible

What is zero trust?

Zero trust is not a product. It's a mindset, a path toward better security that includes a set of core capabilities and use cases. A pathway that requires a strategy, and a set of goals that everyone can agree to. And that's the key-to get agreement across the organization about where to start because many component capabilities can make up a zero trust security approach, but standing on their own, they do not deliver a holistic or efficient solution.

NIST SP 800-207 emphasizes:

An enterprise cannot determine what new processes or systems need to be in place if there is no knowledge of the current state of operations.

- A ZTA deployment involves developing access polices around acceptable risk to the designated mission or business process.
- Before undertaking an effort to bring ZTA to an enterprise, there should be a survey of assets, subjects, data flows, and workflows.

The journey begins by leveraging existing enterprise capabilities

Zero trust requires a comprehensive approach to securing all access across all networks, applications, and environments. Taking a zero trust approach for government enterprises will provide secure access for users, end-user devices, APIs, IoT, microservices, containers, and more—and government enterprises can leverage existing investments in Cisco capabilities for programs like DoD's Comply to Connect (C2C), CISA's Continuous Diagnostics and Mitigation (CDM), software-defined networking, intelligent switching infrastructure, hybrid cloud management, and IoT networking.

Software-defined enterprise – "cross-pillar" benefits

A software-defined enterprise enables the core zero trust logical components as depicted in the NIST model to work together and creates "cross-pillar" advantages and functionalities. In software-defined environment, visibility and analytics will underpin all pillars, as envisioned by the CISA model. Software-defined automation and orchestration support economize, and harmonize, zero trust capabilities and operations across the pillars of user/devices, network/cloud, and application/workload. As seen below, operating across the span of user and devices/networking and cloud/application and data security, and enabled by visibility/analytics and automation/orchestration, Cisco's zero trust capabilities enable government enterprises to take a four-step approach to deliver secure mission outcomes.

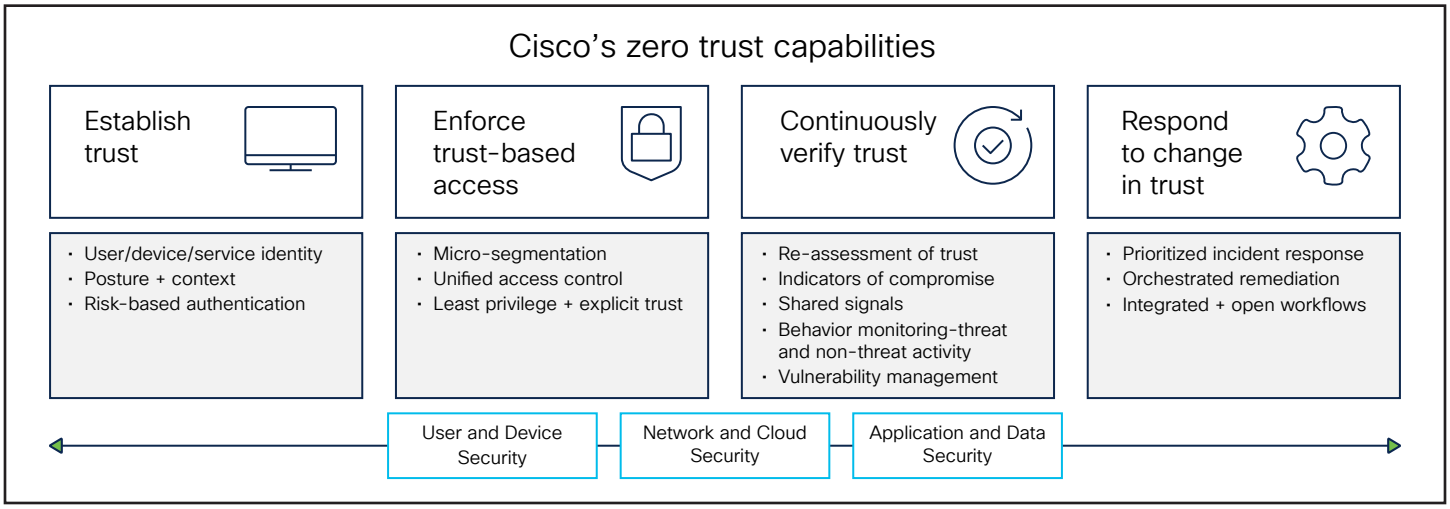

Figure 2. Cisco's zero trust capabilities

Establish trust

Enterprise security must be enabled by visibility into—and have control over—who and what devices are accessing important data. When establishing trust, risk-based authentication requires valid answers to the following:

- Are users who they say they are?
- Are their devices secure?
- Should these applications be communicating with each other?

Zero trust philosophy first establishes and verifies trust for every access request, no matter where it comes from. Trust is not a one-time event; it evolves. Implementing zero trust the right way ensures only the proper users and devices get access when they need it and that threats do not move across the network.

Just as NIST advises, understanding current operational processes including assets, subjects, data flows, and workflows is necessary to develop and deploy access polices that are based on acceptable risk.

NIST 800-207 tenets of zero trust

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including to observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resources authentication and authorization are dynamic and strictly enforced before access is allowed.
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.

Enforce trust-based access

Government enterprises must consistently enforce trust-based access to grant the appropriate level of access and enforce access policies, based on the principle of least privilege. Essential elements are strong identity and role-based access controls, informed with as much dynamic context as possible, along with employment of micro-segmentation based on approved data and application workflows. Automated policy enforcement ensures device posture is continuously verified along with rapid threat containment capabilities. Application access control is automated, including in hybrid operating environments, to enforce secure and approved connectivity between the subject and the requested resource.

Continuously verify trust

Next, change is inevitable, especially when it comes to operating in a dynamic environment. Therefore, trust must be continuously verified by reassessing trust and adjusting access accordingly after initial access has been granted. Visibility/analytics and contextual awareness feed software-defined automation and enable responses to identified vulnerabilities, indicators of compromise, changes in user behavior, or changes of authorization or changes in posture that are not policy compliant. Additionally, helping the user with prompts and direction to understand, self-remediate, and return to compliance not only increases user productivity, but also enhances user experience and decreases help-desk calls.

Respond to changes in trust

Finally, the system must dynamically respond to changes in trust by investigating and orchestrating responses to potential incidents that could compromise devices or data —always keeping a keen watch into suspicious changes in trust level. Rapid response is enabled by integrated threat intelligence, immediate notification of changes in trust, and pinpointing the incident for additional analysis—simultaneously preventing data theft and lateral movement through device isolation and data protection.

Cisco secure platform

Across all pillars of the environment, contextual awareness, visibility, and analytics enable the platform to establish trust, while applying automated, unified policy-based verification and orchestration to empower consistent enforcement of trust-based access.

Steps to Implementing zero trust:

- Establish trust
- Enforce trust-based access
- Continuously verify trust
- Respond to changes in trust

The bridge to possible

The platform

Cisco's zero trust solutions are powered by the Cisco® Secure platform, which includes Cisco's integrated networking portfolio. Our platform enables organizations to make zero trust progress from any starting point.

Across all pillars of the environment, contextual awareness, visibility, and analytics enable the platform to establish trust, while applying automated, unified policy-based verification and orchestration to empower consistent enforcement of trust-based access. That knowledge and understanding enables the platform to continually adapt trust levels based on changing risk and enables automated threat response across networks, devices, and applications to spring back faster in the event of a change in trust. Backed by threat intelligence from Cisco Talos, the platform can see and stop more threats, enabling more rapid and precise response.

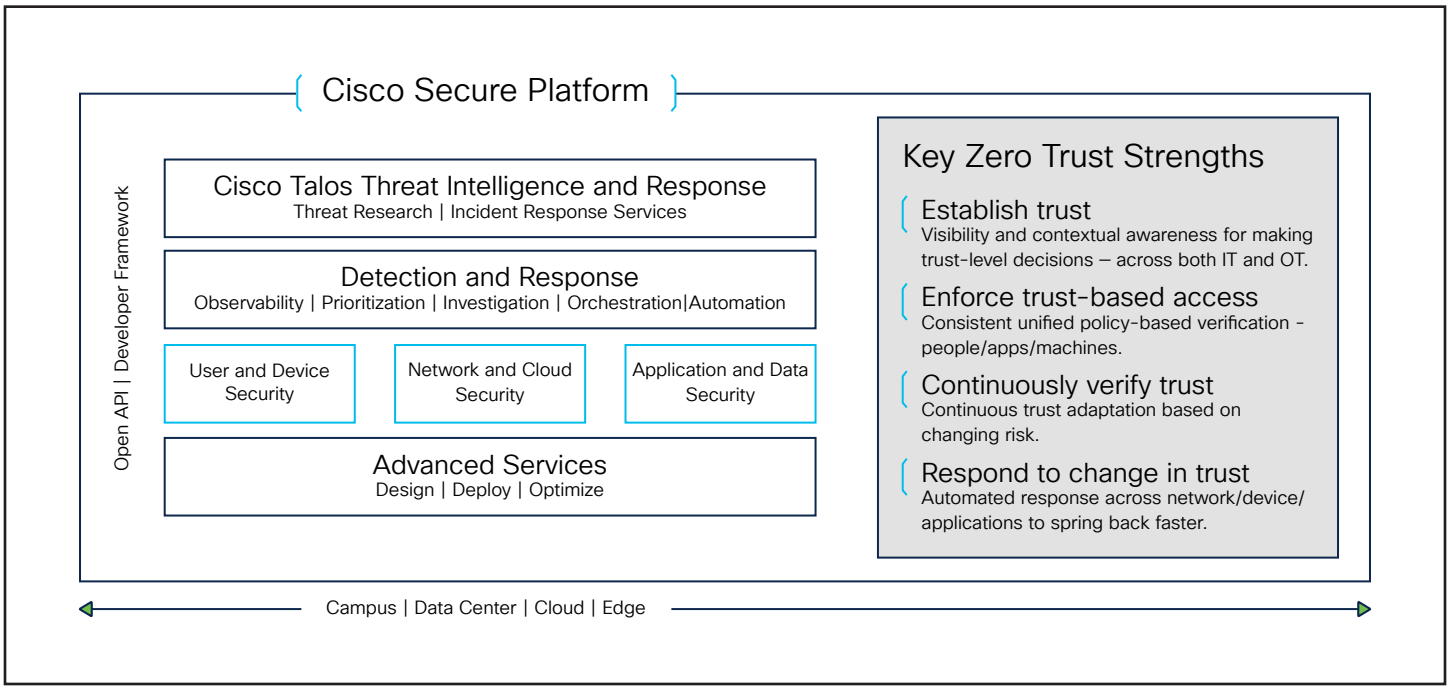

Figure 3. Cisco Secure Platform

The bridge to possible

Where to start

Begin your zero trust journey leveraging investments you have in your enterprise today! Cisco capabilities are designed to work together to share information and enable automation. Cisco offers multiple ways to expand existing investments with an Enterprise Agreement (EA) to enable you to integrate capabilities more rapidly with lower total ownership costs and higher return on investment—Contact Cisco today!

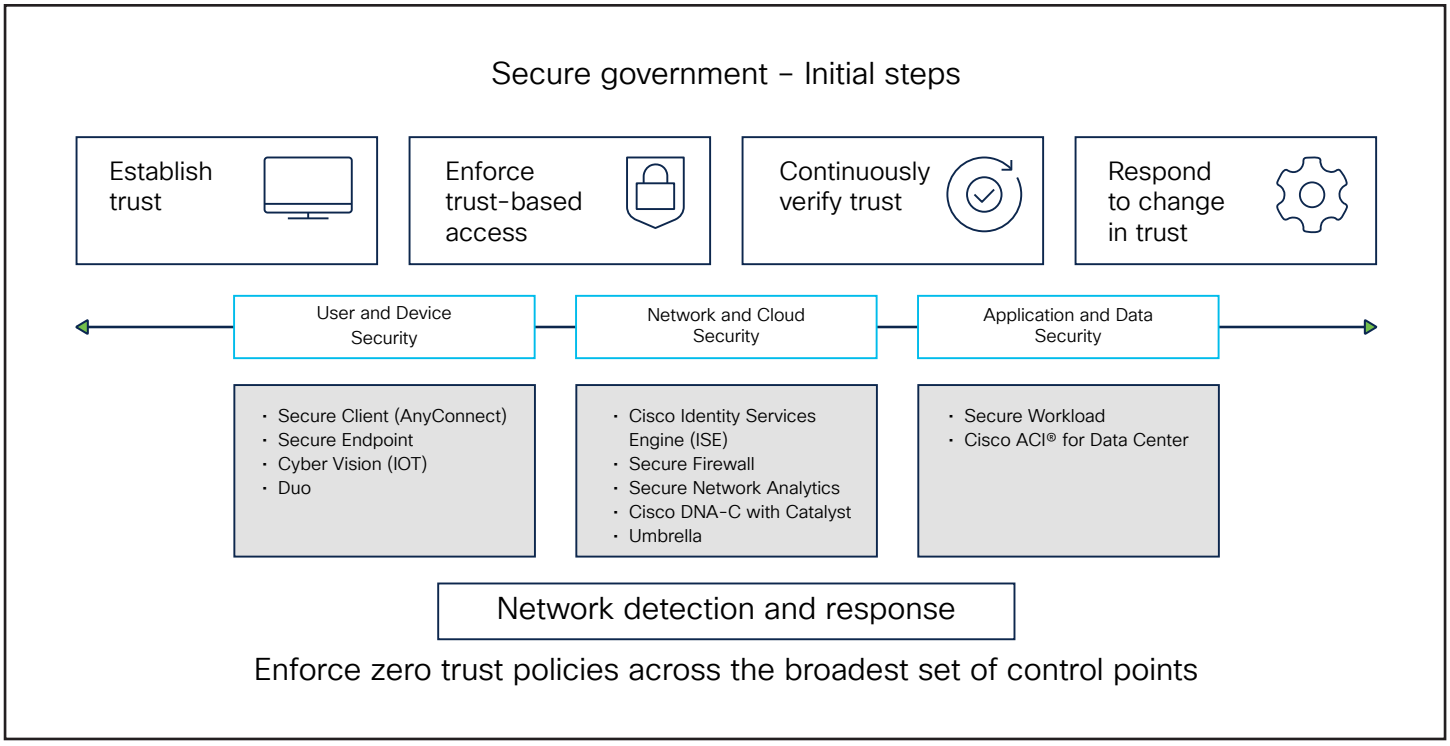

Figure 4. Initial steps to secure government

For more information

To learn more about government and technology, visit cisco.com/go/government and cisco.com/go/securegovernment.

C11-3578323-00 05/23