CISA Zero Trust Maturity Framework

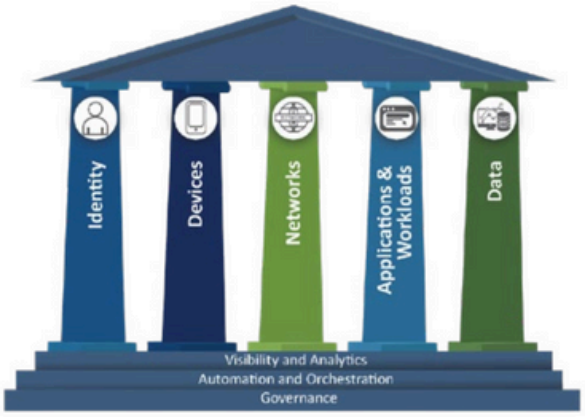
BEYOND IDENTITY

Introduction to the model

Four maturity levels

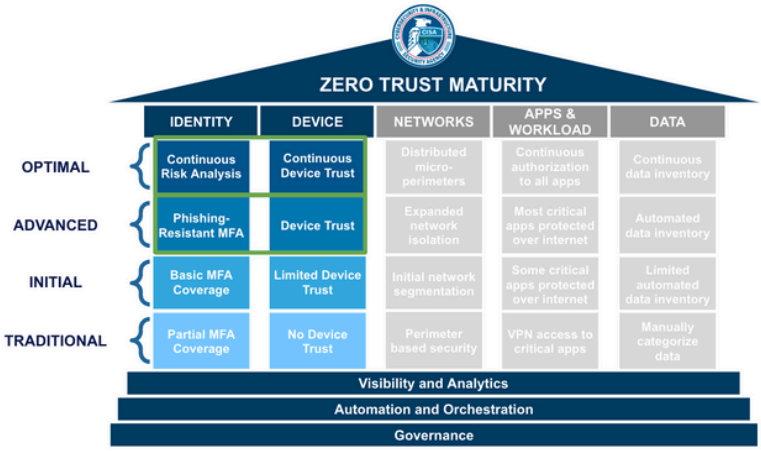
Like many cybersecurity maturity models, CISA's Zero Trust Maturity Model has four levels. The lowest is **Traditional**, which basically means pre-zero trust practices and technologies in areas like authentication, network segmentation, and data management. As organizations acquire more of a zero trust mindset and additional capabilities, they can advance in different areas to **Initial**, **Advanced**, and **Optimal** levels.

It is important to note that an organization does not get an overall status of Traditional, Initial, Advanced, or Optimal. Rather, maturity is assessed for each of the five pillars of the model, so an organization might be able to benefit from advancing to Optimal in one or two areas and to Advanced in another while remaining at the Initial or Traditional level in the remaining pillars.



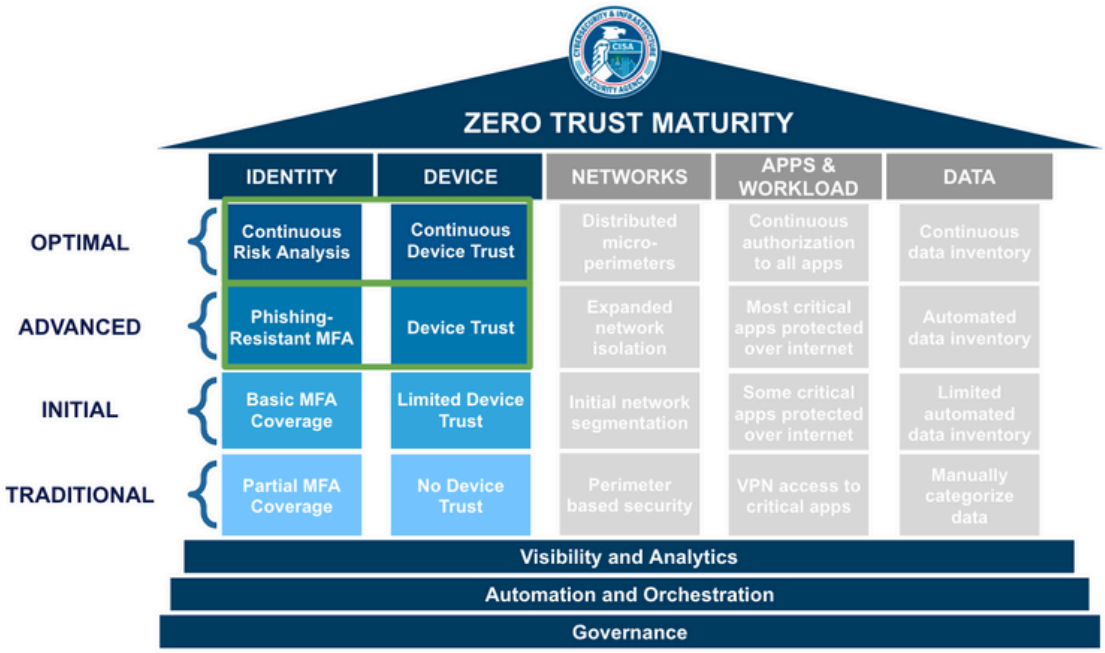
Achieve zero trust maturity quickly with Beyond Identity

Beyond Identity delivers the strongest, continuous identity and device assurance, accelerating the achievement of zero trust maturity for security-oriented organizations.



CISA Zero Trust Maturity Framework

BEYOND IDENTITY



Achieve optimal identity maturity

Beyond Identity enables optimal identity assurance with phish-resistant MFA and continuous authentication using real-time risk signals collected natively from our platform as well as integrated from third-party security tools.

Given that risk changes over time, our platform is uniquely architected to delivers continuous authentication, measured in minutes, that assesses identity security risks even during active sessions.

Not only is access secure, it is also seamless for employees, contractors, and developers to prevent identity-based attacks on your enterprise resources while keeping users productive.

Achieve optimal device maturity

Beyond Identity enables optimal device assurance, as we conduct continuous posture checks on all physical and virtual assets.

Our platform provides customizable, fine-grained device risk query capability for managed and unmanaged devices. This means security and IT teams can collaborate on device risk queries and then enforce continuous, adaptive policies against those risk attributes to enforce

Additionally, our integration with EDRs, MDMs, ZTNAs, SASE, and other security products ensure orchestration and automation across all your security tools, enabling immediate action to restrict any device deemed out of compliance and facilitating real-time risk assessment of devices.

CISA Zero Trust Maturity Framework

BEYOND IDENTITY

Four suggestions for rapid progress

At Beyond Identity, we strongly encourage our customers to adopt the CISA Zero Trust Maturity Model as a tool for creating a step-by-step roadmap toward an effective zero trust architecture. It points CIOs and CISOs in the right direction for:

- More effective cybersecurity through leading-edge technologies and processes
- Increased ease of use and productivity for employees and customers through the adoption of frictionless authentication
- Communicating to executives the goals and progress of their cybersecurity program through the development of practical roadmaps leveraging proven best practices

Based on our experience helping organizations implement zero trust frameworks, we would like to share four suggestions for making rapid gains in maturity.

1. Address the Identity pillar first for fast results and high ROI

Most organizations should focus first on the identity pillar of the model. Getting identity and authentication right is a prerequisite for successfully applying zero trust concepts. Also, you can quickly create big "wins" in security and ease of use.

NIST's operative definition of zero trust begins:

"Zero trust 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." (emphasis added)

As this statement implies, if access decisions are not accurate, the other elements of the zero trust framework won't be effective. If adversaries can capture legitimate credentials and impersonate real users during authentication, then investments in zero trust concepts like authentication for all users regardless of location, continuous verification, and micro-segmented networks lose most of their value.

When renovating a building, you must ensure the foundation is strong before adding new rooms. The elements of the Identity pillar, identity protection and highly accurate authentication, are the foundation of any successful zero trust implementation.

Another reason for focusing first on the Identity pillar is that you can improve maturity quickly for a relatively small investment. For example, in only a few months, you can move from password-based authentication or weak MFA to phishing-resistant MFA and continuous validation and risk analysis. (We'll show you how.) This produces a big "bang for the buck" by strengthening security and employee productivity.

CISA Zero Trust Maturity Framework

BEYOND IDENTITY

2. Link together the Identity and Device pillars early

In version 2.0 of the CISA maturity model, the authors put a great deal of stress on the importance of implementing cross-cutting capabilities so the elements of the different pillars can support and strengthen each other.

This is especially true for linking together elements of the Identity and Device pillars. In particular, our customers have found tremendous value in combining identity and device information to enhance authentication decisions. This includes:

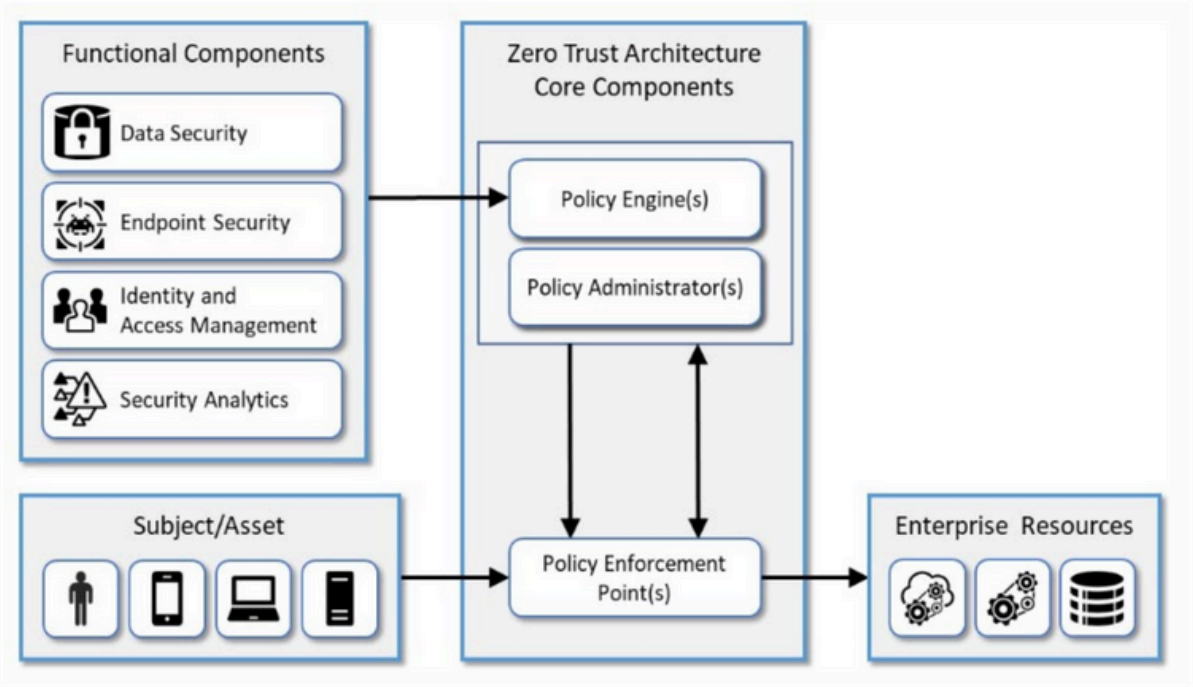
- Checking that devices requesting access to assets are bound to users with permission to access those assets
- Assessing the security posture of devices and restricting access for those that show indicators of risk

At the Initial and Advanced maturity levels, the checks and device assessments might be done only for initial authentications, but organizations can move to the Optimal level by performing them more often for continuous validation and risk analysis.

Also, linking the Identity and Device pillars is another area where organizations can enhance their cybersecurity quickly and relatively easily.

3. Feed your zero trust policy engine with as much security telemetry as possible

A core component of any zero trust architecture is a policy engine that evaluates access requests and determines appropriate responses based on policies specified by the organization (see the diagram below). It is typically part of the organization's authentication solution.



Example of a zero trust authentication policy

If: A device makes an access request

And if: It does not have an active EDR agent on it

Then: Do not authenticate

And: Send an alert to the Security Operations Center

And: Generate a ticket on the IT service management system and notify the user of the need to comply with device security policies

To make optimal decisions about authentication and risk, the policy engine should jointly analyze:

- Credentials from the user or system requesting access to an asset
- Information on the security posture of the requesting device
- Security telemetry (data from security and IT management tools)

We notice that the organizations moving fastest toward zero trust maturity are the ones that take advantage of all the security telemetry they have available from VPNs, endpoint detection and response (EDR), extended detection and response (XDR), and mobile device management (MDM) tools, SIEMs, application protection products, zero trust network access (ZTNA) tools, and other components of their endpoint security and existing security infrastructure.

This capability is called out in Table 5.6 of the CISA model as a characteristic of organizations at the Advanced maturity level for automation and orchestration: "leveraging contextual information from multiple sources to inform decisions." In our experience, an authentication solution that is integrated with a wide range of security tools will perform validation and risk analysis at a much higher level than one that relies entirely on credentials and device information.

4. Prioritize "continuous" and "automated"

If you look at the Optimal maturity level of the high-level model overview on page xx, you will see the words "continuous" and "continuously" several times. That is because collecting and analyzing risk factors only at initial validation is not enough. A threat actor may log on with stolen credentials and only begin performing malicious actions after a period of time. A user might pick up an authenticated device and move it from a low-risk environment (an office) to a high-risk environment (a hotel with dubious WiFi) or might disable the firewall and anti-virus software on the device. Sophisticated adversaries have become very skillful at exploiting gaps between authentication and reauthentication and between device posture checks, which give them a relatively easy way to bypass conventional security controls. Continuous authentication provides ongoing protection and risk management by closing these gaps and by monitoring activities that indicate a potential threat or put the organization at risk. We think it should be an important priority in your zero trust journey.

Our final recommendation is to look for every opportunity to automate. The work involved in collecting, correlating, and analyzing security data generated by thousands of users, devices, applications, and data stores is overwhelming. No human-centered process can hope to keep up. The same applies to responses based on the data. To take actions like stepping up authentication requests and quarantining high-risk systems in time to stop attackers, you need automated workflows that cross the pillars of the zero trust maturity model.