A Practitioner’s Guide to the CISA Zero Trust Maturity Model

How Implementing “Optimal” Identity and Authentication Practices Accelerate the Journey to Zero Trust

Zero trust frameworks: Powerful, but sometimes intimidating

Zero trust frameworks are the cybersecurity industry’s most comprehensive responses to the challenges of defending against attacks on cloud-hosted applications and widely distributed workforces. Thorough, well-designed frameworks have been published by leading analyst firms and standards bodies such as Forrester Research, Gartner®, and the National Institute of Standards and Technology (NIST).

However, zero trust frameworks are complex and, frankly, intimidating to most organizations. They enumerate so many details about zero trust principles, advanced technologies, and re-engineered processes that the desired end state can seem unreachable. And because the frameworks offer little guidance on “what to do first” and “what to do next,” many organizations are deterred from even starting their journey toward a zero trust architecture.

That is where the Zero Trust Maturity Model developed by the US Cybersecurity and Infrastructure Security Agency (CISA) can be extremely helpful. It breaks down the evolution from a traditional starting point to an advanced zero trust architecture into four stages, with specific objectives at each stage. It provides guidance for managers, architects, analysts, and engineers on how to create a customized roadmap of a step-by-step transition from the organization’s current state (whatever that may be) to an optimal end state.

How a maturity model helps

A maturity model lays out successive stages of proficiency that a typical organization will pass through as it advances from a low level of capability toward a full realization of a concept or framework. Usually, maturity models are developed by experts who have observed how enterprises have progressed and the lessons they have learned in the process.

Maturity models serve several purposes. Organizations can them to:

- Assess their current maturity level compared with industry peers
- Construct a practical step-by-step action plan informed by the experiences of other enterprises
- Track progress toward higher levels of maturity
- Calculate costs, benefits, and ROI at each stage of the journey

Good maturity models are not one-size-fits-all. They provide useful guidance but allow each organization to move forward based on its current risk factors, business objectives, and technology infrastructure.

About the CISA Zero Trust Maturity Model

CISA is a US government agency whose mission "is to defend and secure cyberspace by leading national efforts to drive and enable effective national cyber defense, enhance resilience of national critical functions, and advance a robust technology ecosystem." Among other activities, it promotes cybersecurity best practices, disseminates cybersecurity news, advisories, and alerts, and promotes cybersecurity partnerships between public and private sector organizations. CISA is widely seen as the leading authority on how to implement the standards and frameworks developed by NIST (the National Institute of Standards and Technology).

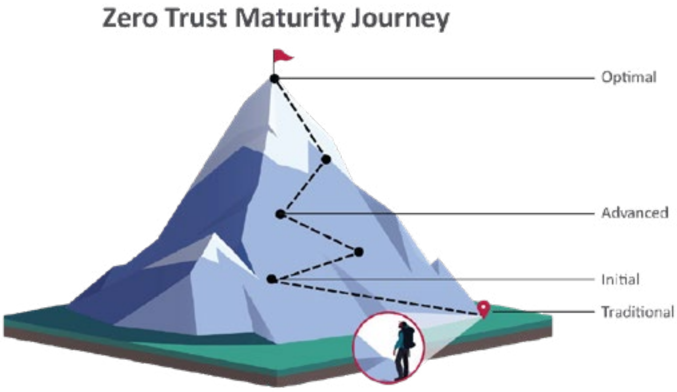
Recognizing that the lack of a maturity model was slowing down implementation of zero trust architectures, CISA published version 1.0 of its Zero Trust Maturity Model in June 2021. It subsequently collected comments on version 1.0 from six trade associations, four federal agencies, 10 consulting firms, 38 technology vendors, and others and used that feedback to publish version 2.0 in April 2023. Many cybersecurity experts agree that the recommendations in version 2.0 are very forward-looking and will undoubtedly influence domestic and international regulators across all industries.

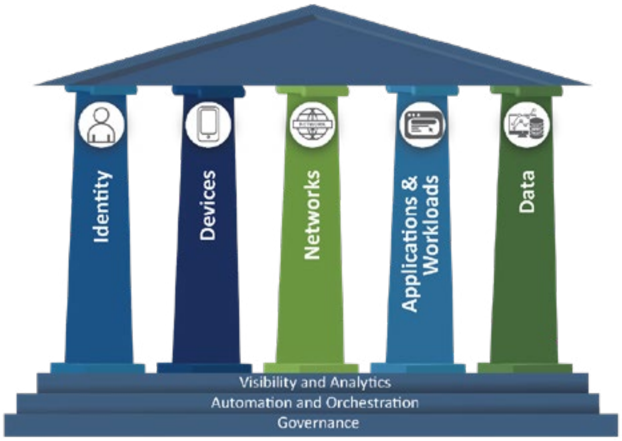
Introduction to the model

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.





Five pillars

A key feature of the model is that it focuses attention on five pillars:

1. **Identity** ("an attribute or set of attributes that uniquely describes a...user or entity")
2. **Devices** ("any asset...that can connect to a network")
3. **Networks** ("an open communications medium including...internal networks, wireless networks, and the Internet")
4. **Applications and Workloads** ("systems, computer programs, and services")
5. **Data** ("all structured and unstructured files and fragments")

The maturity model is essentially about the different levels of "systems, resources, infrastructure, personnel, and processes" needed to protect each of the five object types.

Three cross-cutting capabilities

The model also highlights three capabilities that cut across the five pillars:

1. **Visibility and Analytics** ("observable artifacts that result from...events within enterprise-wide environments" and "analysis [that] can help inform policy decisions, facilitate response activities, and... develop proactive security measures")
2. **Automation and Orchestration** ("automated tools and workflows that support security response functions... and interaction of the development process for such functions")
3. **Governance** ("the definition and associated enforcement of...cybersecurity policies, procedures, and processes")

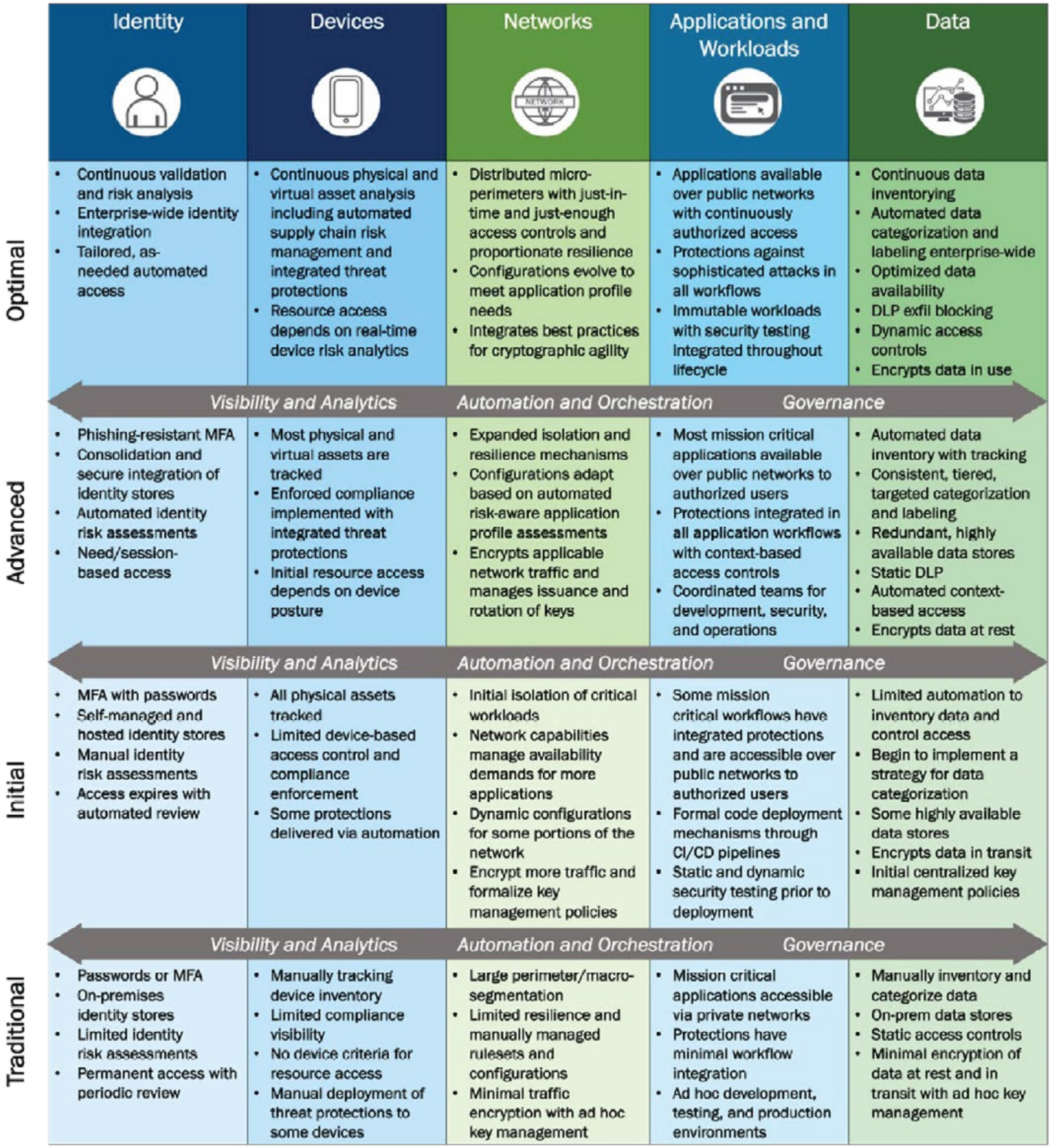
These capabilities are important for increasing effectiveness within each pillar and for supporting interoperability across them, as discussed below.

The high-level model overview and two ways to read it

The authors of the model provide a high-level overview with key details for each pillar at each maturity stage (see the table below). Clearly, it is impossible to absorb all the elements of this table at one glance. However, there are two ways to read it, each of which provides useful insights.

Move up each pillar

By moving up each pillar, you are guided toward a logical sequence of actions for that area. For example, if you read upward in the Identity column from traditional to optimal, you will see how other organizations have stepped up their capabilities for authentication and identity management: from password-based authentication and on-premises identity stores, to MFA with passwords and separate hosted identity stores, to phishing-resistant MFA and consolidated identity stores, to continuous validation of identities and enterprise-wide identity integration (among other progressions).



	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		Automation and Orchestration		Governance
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		Automation and Orchestration		Governance
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		Automation and Orchestration		Governance
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

Identify common themes associated with greater maturity and higher performance

Another way to read the table is to note common themes across all of the pillars that indicate increasing maturity from the Traditional layer to the Optimal layer. These reflect changes in processes, technologies, and mindsets that can lead to order-of-magnitude improvements in metrics such as time-to-detection, time-to-mitigation, and time-to-resolution of issues.

A scan up the chart reveals several common characteristics of maturing organizations, including:

- A transition from one-time validation based on static data to continuous validation and just-in-time risk analysis using real-time data.
- A transition from data captured and analyzed within individual pillars to sharing and using comprehensive data and context across the pillars.
- The increasing use of automation to inventory assets, capture diverse data, analyze risk, enforce policies at scale, and perform many other tasks.

The impact of automation is particularly important. Generally speaking, as organizations advance from the Traditional level to the Initial level they use automation to improve the performance of human-directed processes. As they mature further to the Advanced and Optimal levels, they replace human-directed processes with machine support to machine-directed processes with human support; these steps have a phenomenal impact on productivity, accuracy, and time-to-results.

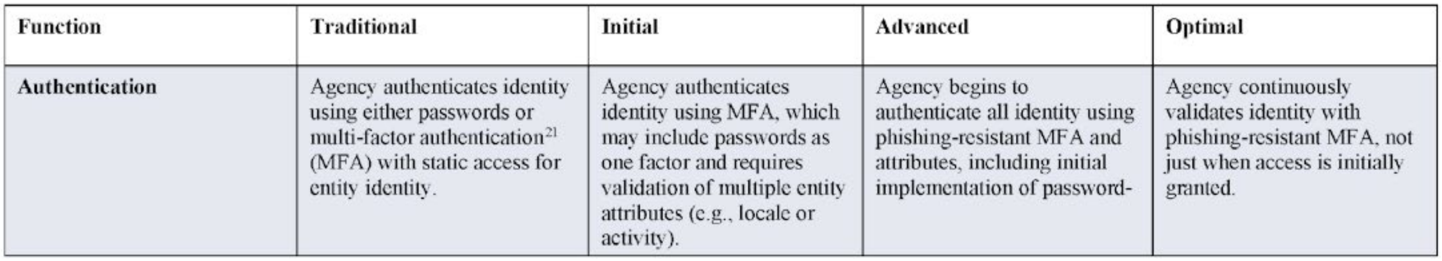
The core of the model: The tables

CISA's Zero Trust Maturity Model does not end with the high-level overview. Six tables go into extensive detail about specific functions related to each of the five pillars and the cross-cutting capabilities.

For example, the table for the Networks pillar lays out how organizations might evolve from traditional to optimal maturity levels for four network-related functions (network segmentation, network traffic management, traffic encryption, and network resilience) and the three cross-cutting functions.

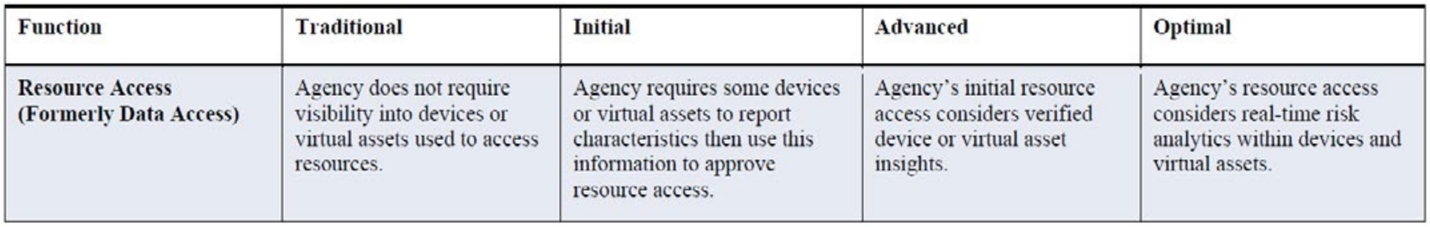
Let's look at the entries for two specific functions.

Authentication is the first function shown in Table 5.1, the table for the **Identity** pillar. You can see from the example below that the model lays out the steps from the Traditional level (password- or very basic MFA-based authentication), to Initial level (MFA with passwords as one factor), to Advanced (phishing-resistant MFA), to Optimal (continuously validated identity with phishing-resistant MFA).



Function	Traditional	Initial	Advanced	Optimal
Authentication	Agency authenticates identity using either passwords or multi-factor authentication[21] (MFA) with static access for entity identity.	Agency authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g., locale or activity).	Agency begins to authenticate all identity using phishing-resistant MFA and attributes, including initial implementation of password-	Agency continuously validates identity with phishing-resistant MFA, not just when access is initially granted.

Resource Access is the third function shown in Table 5.2, the table for the **Devices** pillar. Organizations increasing maturity in this function typically progress from no visibility into devices, to using information from some devices to approve resource access, to verifying the devices at the time of initial resource access, to assessing risks related to the device continuously in real time.



Function	Traditional	Initial	Advanced	Optimal
Resource Access (Formerly Data Access)	Agency does not require visibility into devices or virtual assets used to access resources.	Agency requires some devices or virtual assets to report characteristics then use this information to approve resource access.	Agency's initial resource access considers verified device or virtual asset insights.	Agency's resource access considers real-time risk analytics within devices and virtual assets.

The six tables in Version 2.0 of the model contain a total of 40 such function rows. Together they provide plenty of detail to help cybersecurity managers, architects, analysts, and engineers understand key elements in each pillar and how they progress by maturity level. The authors of the document have been careful to make the descriptions specific enough to be objective and meaningful but not so restrictive as to create artificial or arbitrary requirements.

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.

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:

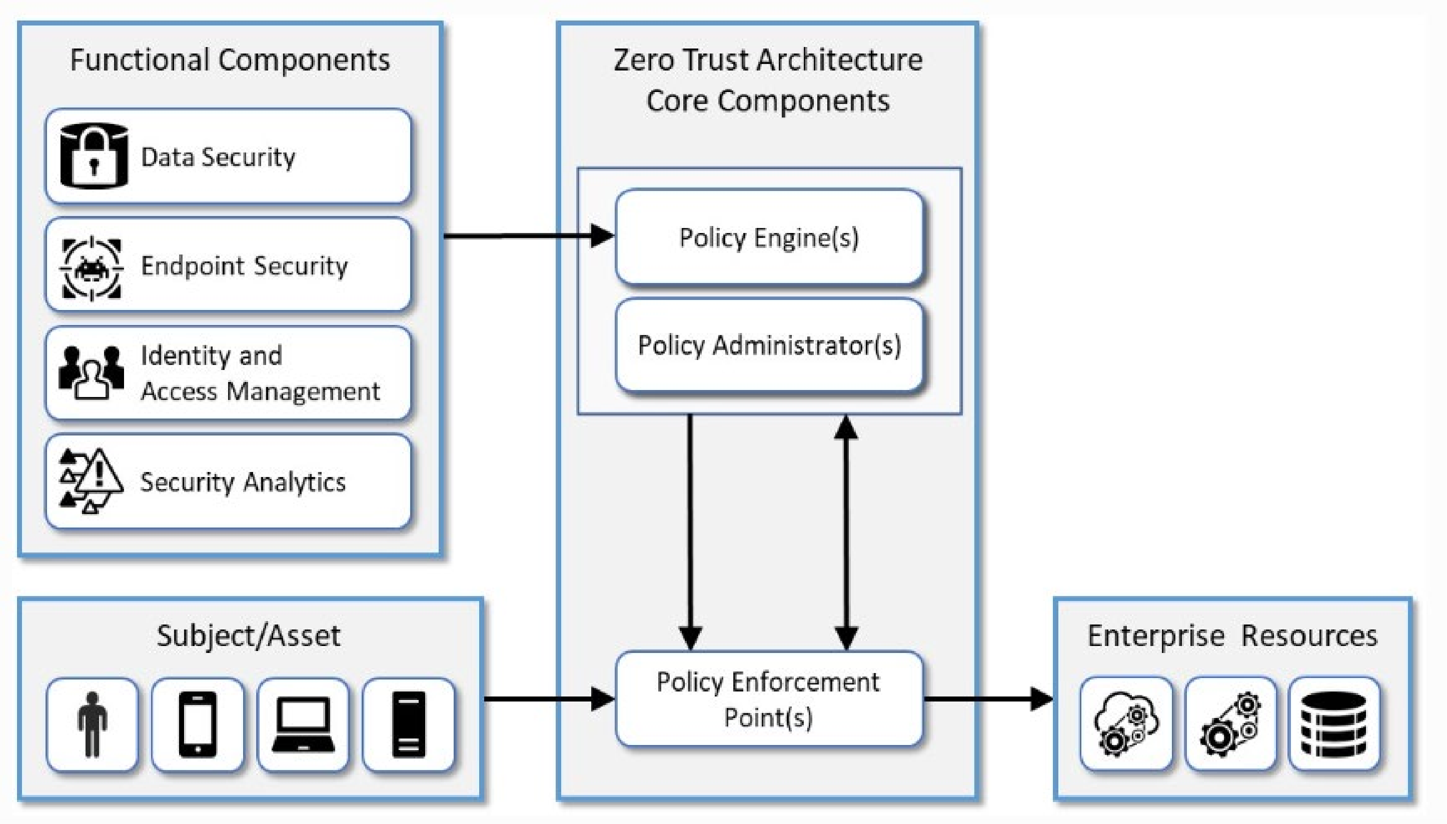
- Checking that devices requesting access to assets are bound to users with permission to access those assets
- Assessing the security posture of devices and restricting access for those that show indicators of risk

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.

To learn more

CISA Zero Trust Maturity Model, version 2.0

NIST Special Publication 800-207, Zero Trust Architecture

Blog post - Dr. Zero Trust on Zero Trust Authentication

Blog post - Zero Trust Maturity Model: Getting Serious About Zero Trust

Blog post - Are You Using Phishing-Resistant MFA? Probably Not

Blog post - How is Continuous Authentication Different from Two-Factor Authentication?

Video: Securing Your Workforce With Zero Trust Authentication

eBook - Zero Trust Authentication: Securing User and Device Access for a Distributed, Multi-Cloud World

Or contact us to talk about the zero trust maturity model and zero trust authentication:
Email address or web form?

BEYOND IDENTITY

Beyond Identity is revolutionizing digital access for organizations looking to improve protection against cyber attacks and deliver the highest levels of security for their workforces, customers and developers. Its suite of passwordless, phishing-resistant, and zero trust authentication solutions improves security and user experience. The platform delivers continuous risk-based authentication incorporating signals from the zero trust ecosystem to ensure only valid users and secure devices gain or maintain access to critical resources. Companies like Snowflake rely on Beyond Identity rely on Beyond Identity's highly available cloud-native platform to thwart attacks and advance their zero trust strategies. To learn more about Beyond Identity's FIDO-2 certified multi-factor authentication (MFA) solutions, visit beyondidentity.com and stay connected with us on Twitter, LinkedIn, and YouTube.