Whitepaper

Zero Trust: Understanding the Identity maturity model

Contents

Zero Trust: Understanding the Identity maturity model

By now, most security practitioners and even security vendors are exhausted from hearing the old adage: “Zero Trust is not any singular technology.” But we shouldn't downplay the importance of the message; emphasizing security best practices and driving Zero Trust adoption are mainstays in executive discussions, including at the board level.

The latest Okta State of Zero Trust report shows “in-flight Zero Trust initiatives” rising from 55% in 2022 to 61% in 2023. While it's a small increase, it's certainly a significant number compared to 2021, when only 24% of companies surveyed were currently working on Zero Trust efforts. As efforts have scaled, so have the understanding and asks of solution providers. Security leaders are well versed in what Zero Trust is and isn’t and well informed about the technologies that support a Zero Trust framework. What security leaders are asking for is a practical approach to implementing Zero Trust. “How do I leverage my technological capability, X, in support of our Zero Trust initiative, Y?” is a frequent ask.

Before we tackle the “how,” we need to levelset and have a mutual understanding of the “what.” As much as Zero Trust benefits from implementing solutions and capabilities, the driving force is the shift in realizing why the concept of trust does not apply to systems. After all, trust is a human emotion that has been incorrectly used to provide attribution to digital systems that operate in a binary realm.

Furthermore, as widely as technologies are inaccurately represented as the solutions for Zero Trust, they exist primarily to connect the elements of people and processes. Instead of applying characteristics reserved for sentient beings, we need to understand that Zero Trust is a strategic framework for promoting a set of security controls that rely less on static, network-based perimeters and instead focus on the Identity, device, and resource pillars. Thus, while technologies are often highlighted as integral to enacting those controls, Zero Trust is just as much about processes. Zero Trust advocates for pursuing three principles: least privilege, no implicit trust, and continuous monitoring. These three principles have associated controls that you can see below in figure1.

Zero Trust Principles

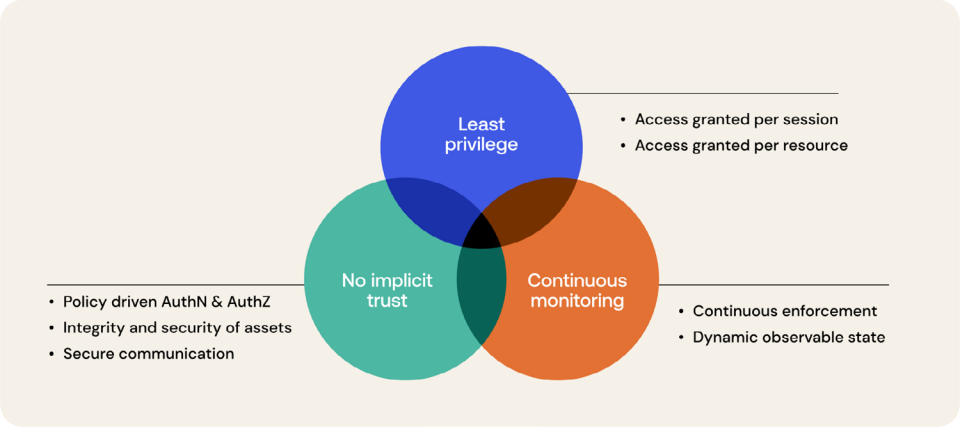

Fig. 1 Fundamental Zero Trust Principles

CISA Zero Trust model

While we can opine on the broader security domain, as the market leaders in Identity and Access Management, we'd be remiss if we didn't give practical guidance on the fundamental pillar of the Zero Trust model: Identity. However, before we outline the aspects of Identity that you should mature over time, we must explain the overall Zero Trust ecosystem. CISA has developed a Zero Trust model that references the pillars of Identity, devices, network, applications, and data as foundational components, with each serving core competencies that deliver security functionality.

The Identity pillar centers around the account requesting access; the devices pillar focuses on the hardware being used; the network pillar looks at traffic as it's en route; the application pillar fulfills the requests and actions invoked; and finally, the data pillar is in charge of acting on the data. These five pillars are further supported by the competencies of Visibility and Analytics, Automation and Orchestration, and Governance that deliver functionality that spans across and stitches together the fabric of Zero Trust. Visibility and Analytics aim for a holistic view of the ecosystem. Automation and Orchestration execute conditional actions. Governance focuses on ensuring allocation of permissions and resources is in compliance. See figure 2 below.

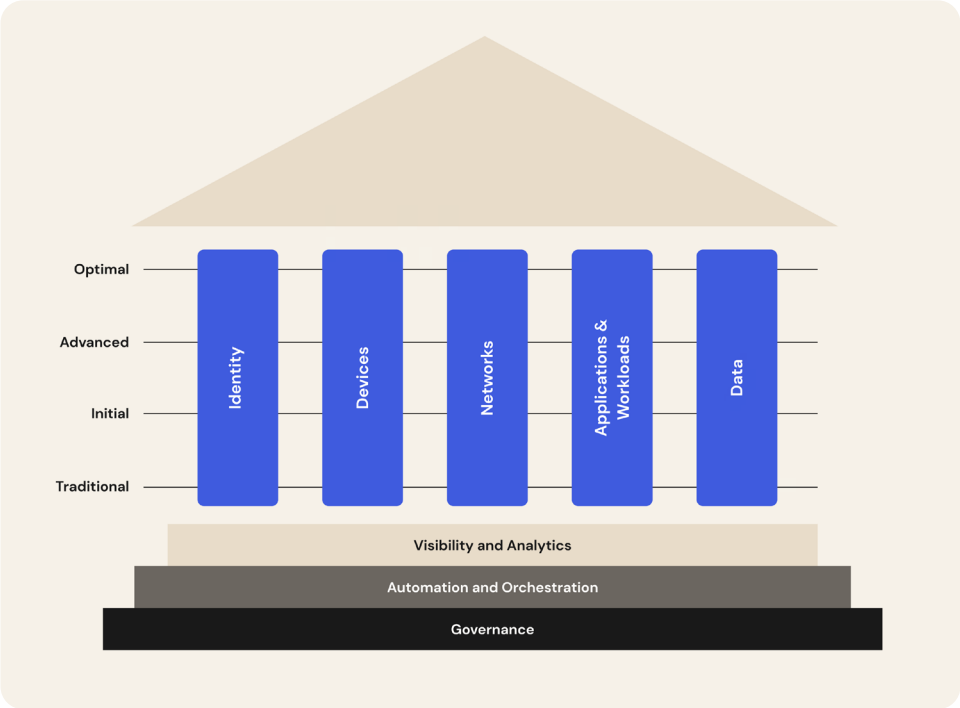

Fig. 2 CISA Zero Trust Model

Identity: Foundational to Zero Trust

In the CISA Zero Trust model, the Identity pillar is introduced first (and rightly so). Identity is core to Zero Trust, as it triggers the entire transaction flow of an entity acting on data; nothing happens from an event perspective until an identity requests to act on data. Identity provides the front-door access to resources and serves as the control plane to ingest, evaluate, and dictate policy. While the other pillars of the CISA model have functional contributions, Identity is the glue that binds the entire model.

On a typical day, a user may log in from different devices, move around different geographies, access different applications, and transact on different data. These dynamic states reduce the explicit impact the devices, networks, applications, and data pillars can contribute for two reasons. Either one of those pillars is absent (when a user doesn't traverse a company network to access resources, maximum enforcement of network layer policies does not occur), or the amount of data available for evaluation is limited (access from a kiosk or public device does not allow for detailed insight into the state of the hardware).

The identity of the user, however, remains static and thus can anchor access control security. Therefore, Identity must serve as the control plane to evaluate signals from all of the components of the CISA Zero Trust model to enforce policy.

See figure 3 below. With Identity an encompassing capability, CISA references the specific controls that reside within the Identity pillar: authentication, Identity stores, risk assessment, and access management. In addition, the previously mentioned Visibility and Analytics, Automation & Orchestration and Governance are included as they provide functionality that spans all of the Identity pillar controls.

The CISA Zero Trust Maturity Model has four stages of maturity for the controls within each pillar: **traditional, initial, advanced, optimal.**

- **Traditional** refers to legacy practices that bring with them technical debt and security gaps, along with manual processes centered on static configurations.
- **Initial** is characterized by a small number of initiatives to start moving off of the traditional controls to scale operations and close security gaps.
- **Advanced** involves shedding legacy controls and embracing modern practices, using automation where applicable. This stage helps eliminate much of the tech debt that plagues traditional environments and starts injecting value through efficiency gains and cost reduction.
- **Optimal** refers to having modern security controls and streamlined (fully automated) processes that deliver continuous functionality, which makes the security teams' job easier and drives business value.

Using these four stages as guides, Identity maturity initiatives aligned to Zero Trust stay on track, and progress is measurable.

Zero Trust Architecture via Identity Powered Security

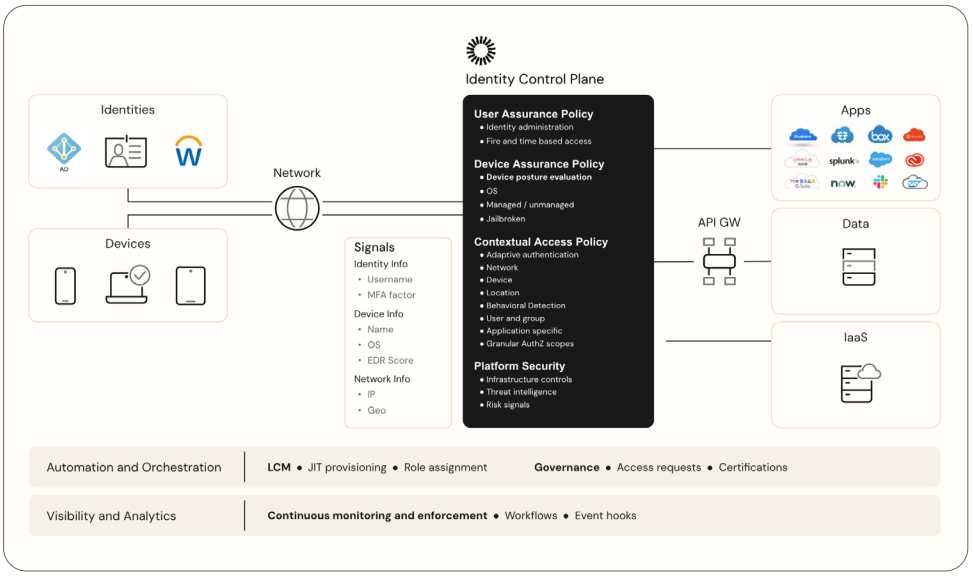

Fig.3 Identity-powered Zero Trust

Authentication

In the Traditional stage, the authentication control is characterized by having a standard password and multi-factor authentication providing static access. Additionally, the second factor is often not strong, resulting in a higher chance of compromise should a threat actor attempt credential theft via brute force, SIM swap, or password stuffing.

Static access represents an attack vector, as credential compromise can lead to account takeover. Additionally, it drastically reduces the effectiveness of a core principle of Zero Trust (least privilege), to grant access expressly to carry out the requested task.

Moving to the initial stage, access becomes dynamic and leverages data context and behavioral analysis during authentication. This improves the security posture, as changes in user profile and context result in the policy's reevaluation.

In the advanced stage, integrating stronger authentication factors and eliminating passwords where possible helps mitigate the threat of MITM attacks and credential compromises. By implementing a strong factor like Okta FastPass, you can introduce phishing-resistant capabilities and eliminate passwords for logging on to applications. This boosts security for the end user and provides them with a seamless, frictionless experience.

At the optimal stage, you leverage the strong controls from the previous stage and integrate continuous validation to ensure the conditions that initially granted access to the identity haven't changed to represent a higher-risk state.

Control	Traditional	Initial	Advanced	Optimal
Authentication	• Legacy protocols • Basic auth • Static access	• Modern auth • Strong MFA • Dynamic access • Some controls still in traditional stage	• Passwordless auth • Phishing-resistant MFA • Fully modernized controls	• Passwordless auth • Phishing-resistant MFA • Continuous validation of user and device state

Identity stores

Identity stores have become prominent components of the tech stack as organizations have taken on digital transformation projects.

While in the traditional stage, environments consist of a user database or active directory maintained on on-prem servers and within the confines of the network.

Those in the initial stage have moved a select few Identity stores to the cloud as workloads migrate to cloud infrastructure. While moving to the cloud offers some gains (i.e. resiliency and redundancy), the burden of self-managing and administrating server fleets still falls on IT teams.

In the advanced stage, IT teams seek to consolidate identities , ideally in a cloud directory like Okta's Universal Directory. This provides the benefit of using cloud-native infrastructure and protocols that shed the gaps left by legacy security.

Finally, in the optimal stage, Identity stores are fully integrated so upstream systems like Identity providers (IdPs) can provide a uniform setting to all users, regardless of where the user identities or systems reside. Organizations can benefit from this capability, as implementing protocols such as SAML or OIDC for logging in to a resource greatly reduces the threat of credential compromise and reliance on basic, forms-based authentication schemes.

Control	Traditional	Initial	Advanced	Optimal
Identity stores	• Disparate user stores • On-prem server farms	• Partial migration to cloud directory • Beginning consolidation of user stores	• Partially cloud-native user directories • Continuously consolidated user stores	• Identity sourced from modern sources of truth (HRaaM) • Fully cloud-native user directory • Complete consolidation of user store

Risk assessment

Often, assessing Identity risks isn't high on the priority list for security teams, a common characteristic of the traditional stage. Primarily, this happens because Identity traditionally belongs to users within the organization, typically existing on a single domain. With a static setup, risk evaluation activities focus on other aspects of the technology stack. As Identity stores expand and move to cloud infrastructure, risk management gains more relevance.

In the initial stage, manual risk assessments are conducted based on static rulesets. Assessments typically involve comparing the values of Identity object attributes and metadata at different points in time. Again, the manual and static aspects of this exercise limit the value provided, as these actions can prohibit real-time risk assessment and inaccurately reflect risk.

In the advanced stage, dynamic policy evaluation and automation help derive risk evaluations that dictate access decisions. This adds value, as security operations can begin to scale and keep pace with environmental changes.

Finally, as an optimal stage configuration, risk assessments happen in real time, based on continuous assessment, resulting in an evergreen protection layer applied to the network.

Control	Traditional	Initial	Advanced	Optimal
Risk assessment	• Small to non-existent risk management practices	• Manual risk assessments • Static rule evaluation	• Dynamic policy enforced • Automation to scale operations	• Real-time risk assessment • Fully automated policy execution

Access management

Access management pertains to how you handle an identity's access to a resource post-authentication.

In the traditional stage, permanent access is authorized for privileged and unprivileged accounts, creating a great deal of security risk in the environment. While these identities have evergreen access to resources, the reliance on ancillary security solutions increases.

In the initial stage, static access remains for general accounts. However, privileged accounts are subject to automated review and timeboxing of their access, resulting in expiration. Without permanent access, sensitive identities must obtain verification after session expiration, which increases security and provides accountability for audit purposes.

In the advanced stage, authorization is temporary, based on methodologies like Role-based access control, and provided on a per-session basis. These methodologies are applicable to standard and privileged access requests. Enforcing per-session controls guarantees that every time a new request comes in, it will be evaluated against the predefined policy and subject to risk analysis.

Enhancing this control further in the optimal stage, you tailor authorization to meet the requestor's needs in a "just-in-time" manner. This practice enforces the principles of no implicit trust and least privilege.

Control	Traditional	Initial	Advanced	Optimal
Access management	• Static access granted • Periodic access reviews	• Static access granted • Automatic access reviews for privilege accounts • Access expirations	• Per-session access • Automatic access reviews for all accounts	• Least privilege access • Just-in-time access

Supporting competencies: Visibility and Analytics, Automation and Orchestration, and Governance

Within the Identity pillar, Visibility and Analytics, Automation and Orchestration, and Governance each deliver specific functionality that has yet to be integrated. As stated earlier, the impact and value of Zero Trust are best realized when the entire ecosystem operates as a cybersecurity mesh; Identity's supporting competencies are integral to making that happen. Delivering functionality spanning the entirety of the Zero Trust model, be it a holistic view, just-in-time actions, or complying with organizational policies, these supporting competencies allow the control plane to have knowledge and enforce actions end to end.

The traditional stage is characterized by all manual processes. Logs are manually analyzed, and any form of joiner, mover, leaver (JML) operations, such as account provisioning and deprovisioning, is manually done and

sourced from segregated Identity stores. Account reviews are manual to support the static policies of Identity assignment.

In the initial stage, event correlation is supported by limited automated analysis. There is some form of automated account setup, although from disparate Identity stores. And there is minimal Automation for Governance activities (such as account certifications).

Moving to the advanced stage, automated log analysis supports log correlation by augmenting events from multiple log sources. JML operations are still partially automated; however, they're now sourced from consolidated Identity stores. Access reviews and certifications are also automated and embedded into the Governance process.

Finally, in the optimal stage, log analysis is fully automated and can be used for behavioral detection purposes, as it comprises multiple log sources the user generates events for. JML operations are also fully automated and reference a consolidated set of Identity stores, allowing for functionality like birthright provisioning, role-based permission allocation, and just-in-time access. Governance activities enhance the security posture by fully automating account review and assignments through continuous assessment and dynamic updates in the form of "just-in-time."

Control	Traditional	Initial	Advanced	Optimal
Visibility and Analytics Automation and Orchestration Governance	• Manual log analysis • Manual JML operations • Manual account reviews	• Automation of log analysis • Partial automation of JML operations from disparate Identity stores • Minimal automation of account reviews	• Automated log analysis of multiple log sources • Partial automation of JML from consolidated Identity stores • Greater automation of account reviews	• Fully automated log analysis across the ecosystem • Fully automated JML operations • Fully automated access requests and reviews

Conclusion: Identity is crucial to Zero Trust

In figure 4, below, you can see a summary of the specific Identity security controls and their stages of maturation. We want to conclude by re-emphasizing that, just as Zero Trust is not a singular technology, Identity is not a singular capability to deliver Zero Trust. While the other capabilities centered around devices, network, applications, and data deliver core Zero Trust functionality, Identity is crucial, as it allows for two-way communication with all the other pillars and across your entire technology stack. Furthermore, the maturity controls matrix exists to recognize that every organization (and every environment) has distinct traits and challenges.

Zero Trust Maturity for Security Controls

	Traditional →	Initial →	Advanced →	Optimal
Authentication	PW+MFA Static Access	PW+AMFA Dynamic Access	PWless+ Phishing Resistant MFA	PWless+ Phishing Resistant MA + Continuous validation
Identity Stores	Self Managed On Prem ID Stores	Self Managed + Cloud Hosted	ID Store Consolidation	Fully Integrated ID Stores
Risk Assessment	Limited ID Risk Mgmt	ID Risk Mgmt via static rules	ID Risk Mgmt via automation and dynamic rules	Risk Mgmt via continuous analysis and dynamic rules
Access Management	Periodic reviews of static access	Automated reviews of static access	Access based on Least Privilege	Access based on Least Privilege and JIT
Visibility & Analytics	Manual log analysis	Log correlation + Automated analysis	Automated analysis + augmented log collection	Comprehensive automated analysis including behavioral
Automation & Orchestration	Fullv manual JML Operations w/ segregated ID stores	Partially manual JML Operations /w segregated ID stores	Partiallv manual JML Operations w/ consolidated ID stores	Fully automation JML Operations w/ consolidated ID stores
Governance	ID policies w/ static enforcement and manual reviews	ID policies w/ static enforcement and minimal automation	Policy automation w/ periodic reviews	Policy automation w/ dynamic and continuous updates

Fig. 4 Identity Security Controls Maturity

Readers can assess their own standing and posture in comparison with the specific stages and the controls within each stage. This assessment will help them set a course for remediation and enhancement. While not every organization is at the same starting point of their Identity maturity journey, all of them should have the same end state in sight. Ultimately, maturing Identity security controls should provide value to the organization and its business initiatives.

Identity certainly meets the criteria when correlating technical efforts with benefits for the organization. It doesn't matter if you're pursuing compliance mandates, making the workforce more agile and productive, enhancing cyber resiliency and defenses to protect crown jewels, or giving stakeholders and shareholders the confidence to continue investing. Zero Trust endeavors should deliver value to the business.