Special Report

Zero Trust Security Strategy: Identifiers and Identity Management

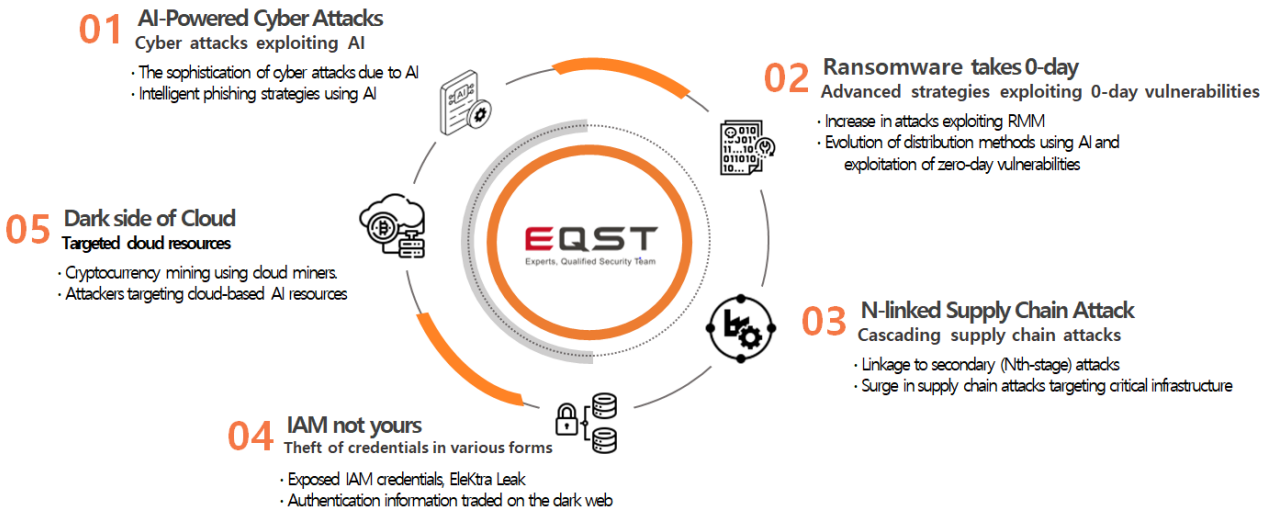
Byung-gwon Hwang / Security SI Business team, Senior Manager

■ Overview of Identity Pillar

The Identifier-Identity Pillar serves as one of the pivotal elements within the Zero Trust architecture, tasked with uniquely identifying and safeguarding all entities, including users, services, and IoT devices. Under the principles of Zero Trust, all users are deemed untrustworthy and must undergo rigorous verification before accessing networks and systems. This process transcends mere initial authentication, encompassing continuous monitoring and the application of dynamic policies to assess the trustworthiness of users and accordingly grant or restrict their privileges.

The Identifier and Identity Pillar distinctly ascertains every entity within an organization, thereby facilitating the consistent application of security policies based on this identification. The process of verifying the identities of users and devices transcends mere authentication procedures, encompassing continual verification and risk assessment. Through this mechanism, organizations are empowered to safeguard sensitive assets from both internal and external threats, and to preemptively prevent security incidents.

In a Zero Trust environment, identifiers and identities serve as both the genesis and the central axis of security, enhancing the security posture through rigorous identity management and access control. Particularly, policies that grant or restrict privileges based on attributes such as a user's role, department, and rank play a pivotal role in actualizing the principle of least privilege. Such policies enable consistent access control across all systems and data within an organization, thereby augmenting the efficiency and reliability of security measures.



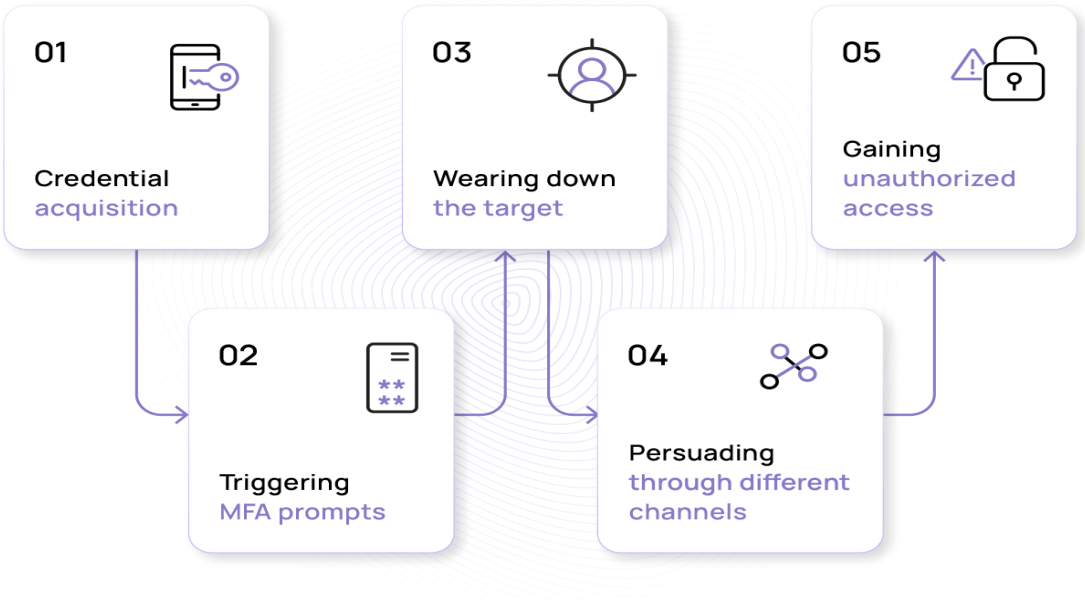
Source: SK Shieldus EQST, "2025 Security Threat Forecast Report"

Figure 1. Review of Security Issues for 2024

According to a recent global threat report, attacks utilizing identities have markedly escalated, positioning them as a primary target for attackers. Notably, Credential Stuffing emerges as one of the most prevalently employed attack methodologies, constituting a significant portion of attack traffic. This technique involves the testing of account information, previously obtained from data breaches, across various platforms using automated tools to illicitly gain access. Such account information is traded on the dark web, serving as a principal means for attackers to attempt initial penetration.

According to SpyCloud's "2025 Identity Exposure Report," it was revealed that during the year 2024, a staggering 53.3 billion pieces of identity data were compromised, marking a 22% increase from the previous year. Such data have been utilized in attacks such as credential stuffing, posing a grave threat to both corporations and individuals alike.

The Multi-Factor Authentication (MFA), a robust enhancement measure within the Zero Trust Architecture, has long been regarded as the standard for protecting identities. However, its efficacy in guaranteeing the security of identities has been compromised due to the emergence of various attack methodologies aimed at circumventing it. These include persistent MFA fatigue attacks, which involve the continuous submission of incorrect MFA credentials, phishing tools utilizing reverse proxy architectures, man-in-the-middle (MitM) phishing, and intermediary attacks that target the storage of MFA credentials. Such diverse tactics underscore the challenges in relying solely on MFA to ensure identity security.



Source: Sosafe, "MFA Fatigue Attack"

Figure 2. Procedure of Multi-Factor Authentication Fatigue Attack

At the current juncture, biometric authentication, reputed to be the most secure method of verification, is not impervious to circumvention. Gartner has projected that by 2026, 30% of enterprises will deem biometric authentication unreliable due to the increasing prevalence of deepfake attacks. In its report "2024 Forecast: AI and Cybersecurity," Gartner referenced the informal detection results of identity verification providers, noting that 15% of fraudulent identity verification attempts are associated with deepfakes, with an indeterminate proportion remaining undetected.

In conclusion, in the context of the escalating prevalence of identity-based attacks, reliance solely on conventional security technologies is no longer adequate. While Multi-Factor Authentication (MFA) and biometric verification remain potent defensive measures, the techniques employed to circumvent these safeguards are becoming increasingly sophisticated. Consequently, it is imperative to adopt continuous monitoring and dynamic policy implementation based on the principles of Zero Trust. Central to the Zero Trust framework are the principles of "continuous verification" and "least privilege." Rather than concluding authentication with a single check, it necessitates ongoing assessment of the user's behavior patterns, connection environment, and device status, thereby requiring additional verification. For instance, should a user access the system from an unusual location or engage in atypical activities, it would be prudent to demand further authentication steps or restrict their access rights. Furthermore, even after identity verification through MFA and biometric checks, limiting users to only the essential privileges needed for their tasks can significantly reduce the attack surface. This approach not only restricts users from accessing sensitive data or systems unnecessarily but also minimizes the risks associated with insider threats and the abuse of privileges.

Ultimately, organizations must fortify their identity protection systems through a multifaceted approach that encompasses the adoption of Zero Trust-based passwordless authentication, the enhancement of user behavior analytics and risk assessment, and the augmentation of biometric verification. By implementing these strategies, organizations will be able to safeguard sensitive assets effectively within an increasingly sophisticated threat landscape and establish a reliable digital environment.

■ Key Elements of the Identifier·Identity (Identity) Pillar

In the architecture of Zero Trust, the Identity pillar serves as a pivotal domain that addresses all security elements related to users, playing an indispensable role in the implementation of Zero Trust principles. Users are not merely individuals but encompass various forms such as service accounts and IoT devices, and the identification and verification of these entities constitute the foundation of the security framework.

Particularly in a Zero Trust environment, all users are considered untrustworthy entities, necessitating continuous verification and the implementation of least privilege to control access. To facilitate this, identity and credential pillars encompass various elements including user inventory management, account and permission administration, enhanced authentication, and risk assessment, each playing a pivotal role in fortifying an organization's security posture.

Below, we meticulously examine the principal components of identifiers and identity pillars, alongside the administrative and technical measures necessary for their implementation.

1. User Inventory

The user inventory serves as the fundamental starting point for identifying and managing all users within an organization. In a Zero Trust environment, it is imperative to precisely identify users and maintain their identities in an up-to-date state. The user inventory provides information on who within the organization has access to specific assets, thereby facilitating efficient management of access control and authorization.

Users manage their data through a continuously updated catalog of information. This catalog must encompass not only the users' basic details but also their identity information. In the initial stages, this data may be managed via files or manually, but as maturity increases, it becomes imperative that an automated system updates user information in real time. Furthermore, based on reliable data, permissions should be capable of being automatically modified.

Users must be grouped according to department, position, and role, and this group information should be automatically updated whenever there is a change in a user's status. This mechanism restricts access to assets solely to those required by users belonging to specific groups.

2. User Account Management

User account management constitutes a system that enables each user to access resources through the accounts they possess. Account management transcends mere creation and deletion of accounts; it necessitates centralized control and administration throughout the entire lifecycle of an account.

Each user must be assigned a unique account, which is to be catalogued and administered centrally. In the initial stages, it is feasible to manage accounts simply through files or manually, yet there should be a progression towards the adoption of an integrated system such as Identity Credential Access Management (ICAM). This system would facilitate the centralized and uniform management of all accounts.
It is imperative that the entire process, from the creation to the deletion of user accounts, be automated to prevent the misuse of unnecessary privileges. Particularly, it is essential to establish a system that continuously verifies the status of accounts based on users' trustworthiness data, utilizing artificial intelligence and machine learning, and automatically adjusts permissions when necessary.

3. Management of User Passwords

Passwords serve as the fundamental method of authentication in numerous systems. Consequently, the management of passwords is an essential component of system security. A robust password policy must encompass requirements for periodic changes and complexity regulations, in addition to implementing supplementary security measures to prevent the loss or theft of passwords. Users are required to periodically update their passwords, and such mandates should be automatically communicated by the system. In organizations of higher maturity, passwords can be automatically updated, and users may verify their new passwords through a verification process.

Passwords must be configured to meet complexity requirements in accordance with policy. This policy enforces compliance among all users. Additionally, in the event of password loss, a lockout policy should provide enhanced security, and a system must be established to respond immediately when anomalous activities are detected.

In the Zero Trust architecture, it is recommended not only to manage passwords but also to actively utilize additional authentication or Multi-Factor Authentication (MFA) based on user behavior. This approach is adopted to augment the security that is otherwise insufficient with the mere use of passwords, by continuously evaluating the user's access environment and behavioral patterns, and demanding additional authentication procedures when necessary. For instance, if a user accesses from an unusual location or engages in abnormal activities, security can be reinforced through MFA.

Ultimately, the transition to a Zero Trust architecture aims to adopt a Passwordless approach. This strategy fundamentally resolves the issues of password reuse and the risks of breaches by leveraging robust authentication technologies such as biometric verification (fingerprint, facial recognition), FIDO2 tokens, or physical keys. The Passwordless method not only enhances user experience but also effectively strengthens security, becoming increasingly crucial within a Zero Trust environment.

4. User Privilege Management

In a Zero Trust architecture, the principle of least privilege is of paramount importance. User privilege management aims to restrict each user's access solely to the minimal resources necessary for the execution of their duties.

Access permissions for each system and resource must be individually configured, and these permissions require periodic review and updates. Furthermore, access permissions should be differentiated according to various roles such as operators and administrators within each system. It is imperative that permissions to access and modify resources are clearly defined for each resource.

All activities performed by users accessing resources must be monitored in real-time, and a system that immediately blocks or provides warnings upon detection of any anomalous signs is essential.

5. User Authentication

In a Zero Trust environment, mere reliance on IDs and passwords is insufficient. User authentication must be robustly enhanced, incorporating Multi-Factor Authentication (MFA) to bolster reliability.

Identity Federation is a system that enables access to multiple services with a single login (utilizing standards such as SAML, OAuth, etc.). By establishing an enterprise-wide Identity Federation system, it is possible to undergo a consistent authentication process across all systems and applications.

Multi-Factor Authentication (MFA) furnishes an additional layer of security and necessitates the fortification of authentication procedures based on data used to assess trustworthiness. MFA secures user authentication more robustly by amalgamating knowledge-based (passwords), possession-based (One-Time Passwords, OTP), and biometric-based (fingerprint) elements.

6. Integrated ICAM Platform

The Integrated ICAM (Identity Credential Access Management) platform serves as a pivotal component within the Zero Trust architecture, performing the role of centrally managing access control and credentials for all resources. ICAM, an expanded concept of the traditional IAM (Identity and Access Management), transcends mere identity management by encompassing credentials as well, thereby enabling a more refined assessment of the trustworthiness of users and entities.

The ICAM platform centrally manages all user-related information, thereby automating the processes of credentialing and authentication. It employs Role-Based Access Control (RBAC) to automatically grant or restrict access to resources based on each user's role. Furthermore, it utilizes Attribute-Based Access Control (ABAC), enabling the application of dynamic policies that consider various contexts such as the user's location, device status, and behavioral patterns.

ICAM utilizes the Policy Information Point (PIP) to ascertain user credentials based on data conveyed from systems such as Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and Unified Endpoint Management (UEM). This information facilitates the real-time analysis of user behavior patterns and device states to assess risk levels, thereby enabling continuous authentication and verification processes. For instance, should a user engage in anomalous network activities or contravene security policies, the ICAM platform can promptly generate alerts or demand additional authentication procedures.

ICAM is also intertwined with Privileged Access Management (PAM), thereby enhancing identity-based credentials through the control and monitoring of privileged account access. The integration with PAM stringently restricts access to sensitive systems and data, playing a pivotal role in thwarting insider threats and the misuse of authority.

7. User Risk Assessment

In a Zero Trust environment, it is imperative to assess the risk level of each user and dynamically adjust security policies based on this evaluation. The risk level of each user is quantified and assessed based on compliance adherence and the detection of anomalous behaviors.

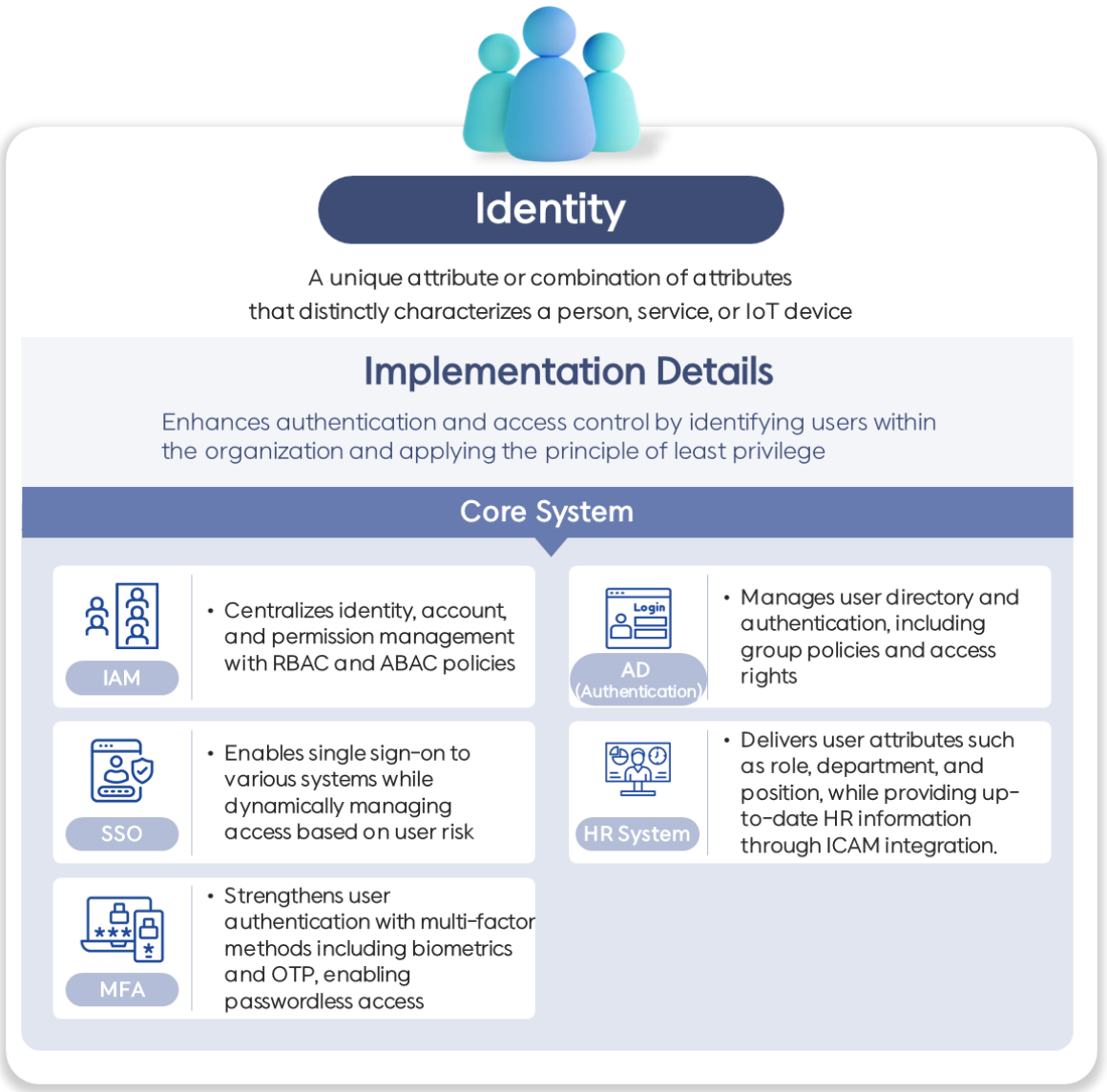
Risk assessment is utilized as critical data for the enhancement of authentication and the authorization process, and it must facilitate immediate responses through real-time monitoring.

Identifiers and identity pillars play a pivotal role in safeguarding sensitive assets within an organization and effectively thwarting both insider threats and external attacks. Furthermore, they furnish both flexibility and reliability to adapt to the evolving threat landscape, and are crucial in implementing consistent security policies within a zero-trust environment and establishing a sustainable digital security framework. Through these measures, organizations can maintain a more robust and reliable security posture, thereby fostering a secure digital environment.

■ Implementation of Zero Trust Features by Key Systems

To successfully implement a Zero Trust environment, both technical solutions and systems capable of executing these solutions are imperative. The Zero Trust architecture is predicated on the principle of "never trust, always verify." To actualize this, a system that can authenticate and continuously verify the identities of users and entities, and ensure minimal privilege access, is essential.

The systems listed below each play a pivotal role from the perspective of identifiers (Identity) within a Zero Trust environment, and their interconnectivity can fortify an organization's security posture. It is essential to examine the specific functions that each system must perform to implement a Zero Trust environment, as well as the enhanced security benefits that the organization can achieve through these implementations.



Source: SK Shieldus, "The Initiation of Zero Trust: Completion through SKZT"

Figure 3. Principal Systems for Identifiers and Identity Verification

1. SSO (Single Sign-On)

Single Sign-On (SSO) is an integrated authentication system that enables access to multiple applications and systems through a single verification, thereby securing both user convenience and operational efficiency. However, in a Zero Trust environment, mere user convenience is insufficient; instead, a security capability that allows for continuous verification and dynamic control is imperatively required.

In a Zero Trust environment, Single Sign-On (SSO) transcends the mere level of single portal authentication. It must support integrated authentication for various access routes, encompassing not only web environments but also interconnections with cloud services such as AWS, Azure, and GCP, as well as client/server-based internal systems. It is a fundamental premise that each environment meets its specific authentication requirements through the adoption of standard authentication protocols (such as SAML, OAuth, and OIDC), thereby ensuring interoperability and scalability.

Within the framework of Zero Trust principles, Single Sign-On (SSO) transcends its conventional role of merely handling initial authentication. Post-initial authentication, it is imperative that SSO continuously analyzes a plethora of contextual information in real-time—such as the validity of the session, alterations in user behavior, the devices and locations of access, IP addresses, and timing of access—to detect potential manipulations of authentication values. Subsequently, it must be capable of executing necessary follow-up actions, including re-authentication or session termination. In this process, encryption of authentication tokens is fundamental. Moreover, the architecture must incorporate technologies designed to prevent the alteration or forgery of authentication values, thereby proactively countering attempts at session hijacking and similar attacks.

Furthermore, rather than employing a simplistic, static rule-based approach for user authentication, it is imperative to implement a flexible policy configuration that performs risk scoring based on multiple factors (such as device type, connection location, time zone, and IP characteristics). This allows for the dynamic adjustment of authentication levels or even the alteration of the authentication pathway itself. For instance, even if possessing identical credentials, additional authentication measures (such as Multi-Factor Authentication, MFA) or access restrictions should be concurrently applied when a user logs in from an unusual location, during a suspicious time period, or using a new device.

All such authentication activities and access flows must be monitored in real-time through a visualized dashboard, which systematically reports on the history of authentication successes and failures, individual user access records, and the occurrence of risk events. This transcends mere security surveillance, serving as crucial foundational data that can be utilized not only for User and Entity Behavior Analytics (UEBA) but also for the reinforcement of security policies.

Ultimately, Single Sign-On (SSO) transcends the mere category of a simple authentication system, establishing itself as a real-time security operational infrastructure that provides a sustainable verification system for users and entities, serving as the 'initial gateway' in a zero-trust environment. The technical and managerial sophistication of this system is of paramount importance in the zero-trust architecture, to the extent that without a properly implemented SSO, even the starting point of the zero-trust architecture is difficult to establish.

2. Identity and Access Management (IAM)

Identity and Access Management (IAM) serves as a pivotal component within the Zero Trust architecture, centralizing the management of user accounts and permissions while bolstering security controls through its integration with various business systems. IAM transcends mere account registration and deletion, implementing granular access control linked to user identities and permissions. This facilitates the continuous enforcement of the principle of least privilege.

In a Zero Trust environment, Identity and Access Management (IAM) must be equipped with integration capabilities with various directory systems such as LDAP, AD, and DB File to link diverse data including personnel information and user attributes. It should also support standard protocols (SAML) and API integrations to ensure flexible integration with heterogeneous systems including web-based, client/server environments, and cloud platforms. Through these mechanisms, organizations are able to centrally manage user accounts and permissions across all business systems, and automate tasks such as the detection of policy-violating accounts and the cleanup of dormant accounts, thereby maintaining continuous appropriateness of permissions.

Particularly, under the principles of Zero Trust, it is imperative to intricately implement policy models such as ABAC (Attribute-Based Access Control) and RBAC (Role-Based Access Control). These models should enable permission control based on a variety of attributes including the user's role, department, location, and connection environment. The configuration of such role-based and attribute-based permissions transcends the limitations of manual administration by managers and necessitates the incorporation of policy automation features facilitated by Artificial Intelligence or machine learning.

Predictive-based access right recommendations, detection of permission conflicts, and anomaly-based policy restructuring are not merely theoretical functionalities but are, indeed, core features currently implemented in commercial IAM products. For instance, certain global IAM solutions learn from users' past access patterns and job histories to automatically suggest appropriate permissions when integrating with new business systems, or they detect excessive permissions by comparing them with those of similar job roles.

Additionally, anomaly detection engines based on machine learning generate alerts or automatically reduce permissions when user behavior deviates from the typical workflow. These functionalities are transforming Identity and Access Management (IAM) from a mere account management system into an 'intelligent access control hub', thereby substantially enhancing the efficacy of implementing a zero-trust security framework.

When expanded, IAM systems can evolve into ICAM (Identity, Credential, and Access Management), which incorporates credentials and serves as a pivotal integrated system based on zero-trust principles. ICAM interfaces with various Policy Information Points (PIPs) such as EDR (Endpoint Detection and Response), UEM (Unified Endpoint Management), Micro-Segmentation, SIEM/SOAR (Security Information and Event Management/Security Orchestration, Automation, and Response), DLP (Data Loss Prevention), and DSPM (Data Security Posture Management). This integration facilitates the real-time assessment of trust levels for users and devices, subsequently enabling the application of dynamic access policies. Consequently, IAM transcends its traditional role of mere authentication and account management to become a 'core system' foundational to the zero-trust environment.

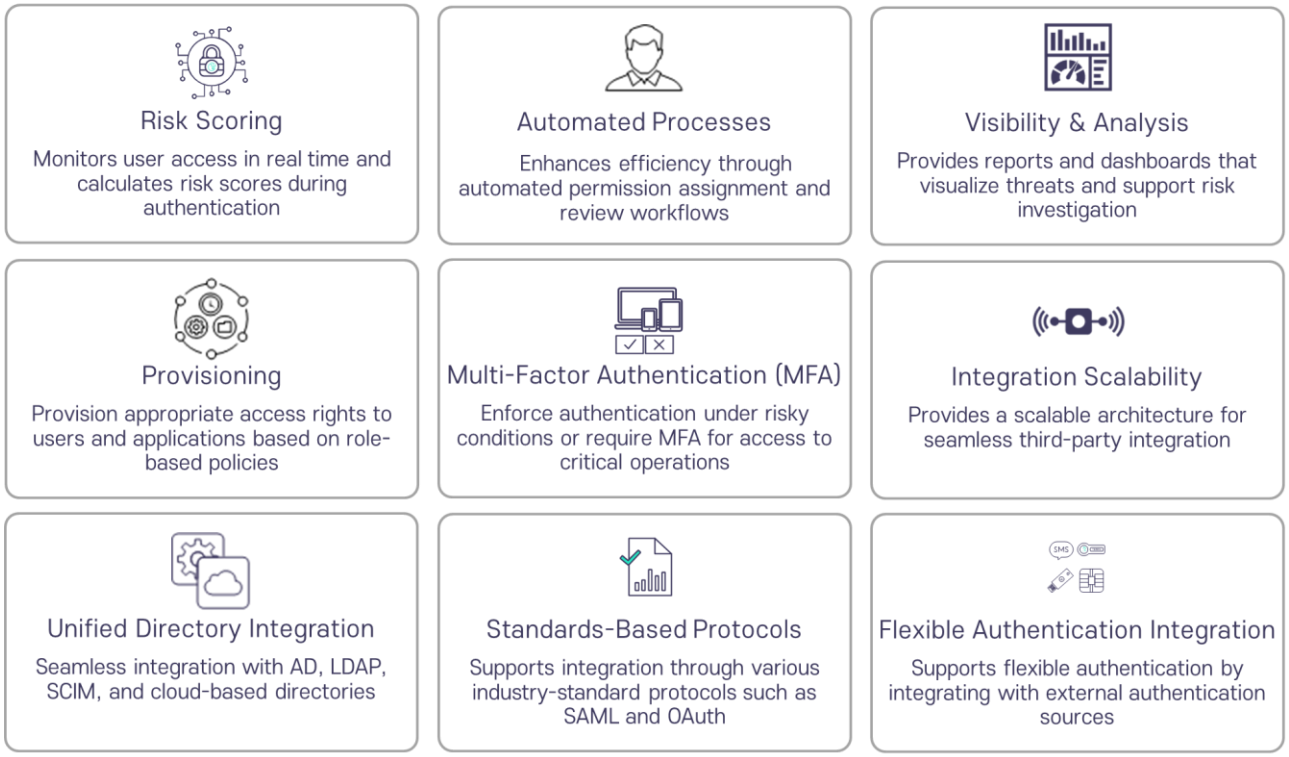


Figure 4. Key Features of Zero Trust-Based SSO/IAM

3. MFA (Multi-Factor Authentication)

Multi-Factor Authentication, commonly abbreviated as MFA, represents a sophisticated security protocol that necessitates the presentation of two or more verification factors to gain access to a resource such as an application, online account, or a VPN. This method is an enhancement over traditional single-factor authentication (SFA), which typically relies solely on a password or PIN. MFA increases security by requiring multiple forms of evidence, which are categorized into something the user knows (password or answer to a security question), something the user has (a trusted device that cannot easily be duplicated, like a phone), and something the user is (biometrics, such as fingerprints or facial recognition).

The implementation of MFA is crucial in fortifying the security defenses of an organization, particularly against the backdrop of escalating cyber threats and sophisticated hacking techniques. By integrating MFA, organizations can significantly mitigate the risk of unauthorized access, thereby safeguarding sensitive data and systems from potential breaches. This multi-layered approach ensures that even if one factor is compromised, the presence of additional barriers can prevent malicious access, thereby providing a robust security framework that aligns with contemporary cybersecurity standards.

Multi-factor Authentication (MFA) serves as a pivotal instrument in actualizing the principle of 'continuous verification' within a Zero Trust environment, enhancing security by amalgamating various authentication methods rather than relying on a singular approach. Notably, while MFA is often integrated with Single Sign-On (SSO) functionalities to operate as a unified authentication platform internationally, the domestic security landscape typically features MFA as an independent, standalone authentication system. This architectural distinction presents both advantages and disadvantages in terms of system flexibility and the segregated operation of security policies, necessitating careful consideration of both aspects within a Zero Trust framework.

Multi-Factor Authentication (MFA) systems fundamentally operate by implementing additional verification measures when anomalous user activities are detected within Single Sign-On (SSO) and Identity and Access Management (IAM) frameworks. A plethora of methods are employed, including One-Time Passwords (OTP), hardware/software tokens, and mobile-based biometric authentication (such as FIDO2-compliant fingerprint and facial recognition). These authentication modalities are designed by integrating the foundational principles of information security authentication: Type 1 (Knowledge), Type 2 (Possession), and Type 3 (Inherence). The essence of multi-factor authentication lies in the synergistic complementarity of these composite authentication elements, which serves to mitigate authentication threats.

Recently, Multi-Factor Authentication (MFA) technology has transcended its traditional role as a mere means of authentication, evolving significantly. For instance, subsequent to the advent of FIDO2, there has been a continuous discourse on the development of next-generation technologies focusing on enhancing the interoperability of authentication across browsers and devices, bolstering the security of biometric authentication, and simplifying authentication processes. Particularly, the technology of Liveness Detection in biometric verification processes is being employed to detect fraudulent attempts such as deepfakes or recorded videos. Moreover, there is an emerging trend towards the application of next-generation cryptographic algorithms, such as Post-Quantum Cryptography (PQC), in the issuance and transmission of authentication tokens. Thus, MFA is establishing itself as a pivotal technology in countering sophisticated authentication threats, moving beyond simple authentication procedures to strengthen its role as a precise authentication gateway within the Zero Trust architecture framework.

Consequently, Multi-Factor Authentication (MFA) does not treat user authentication as a one-time event; rather, it provides a continuous and dynamic authentication system through mechanisms such as Risk-Based Authentication (RBA), behavioral re-authentication, and context-based policy enforcement. This transcends mere login procedures, continuously assessing and fortifying trust, thereby functioning as a pivotal component of the Zero Trust model. Moreover, through its close integration with Single Sign-On (SSO) and Identity and Access Management (IAM), MFA has established itself as a sophisticated security infrastructure that meticulously verifies user identities.

4. Active Directory (AD)

Active Directory (AD), a directory service provided by Microsoft, stands as the cornerstone system for centrally managing user accounts, groups, devices, and policies within the most prevalently utilized Windows-based infrastructure environments. Despite its status as a legacy system with a lengthy history, it continues to serve as the principal infrastructure for user authentication and access control in the majority of corporate settings. Particularly noteworthy is the rapid proliferation of hybrid environments constructed through the integration of on-premises AD and Microsoft's cloud-based directory service, Entra ID (formerly Azure AD). This integration exemplifies a significant trend in the evolution of enterprise IT infrastructure, facilitating a seamless blend of local and cloud functionalities.

Active Directory (AD) transcends the mere function of a user repository, acting as an information hub that, within an organization, interlinks with various systems such as SaaS applications, file servers, and ERP systems, providing real-time user identity information, group attributes, and authorization policies. Particularly, numerous security systems including Single Sign-On (SSO), Identity and Access Management (IAM), Endpoint Detection and Response (EDR), and Unified Endpoint Management (UEM) rely on AD to interpret user permissions and dynamically apply access control policies. Consequently, the accuracy and currency of AD information are pivotal factors that determine the reliability of the entire security framework.

In a Zero Trust environment, Active Directory (AD) is inherently a security subject and simultaneously a target for attacks. Following initial intrusion, attackers prioritize AD to facilitate privilege escalation, engaging in actions such as administrator account theft, authority expansion, and securing service access pathways within AD itself. Indeed, numerous breach incidents have demonstrated that AD has been exploited as a conduit for privilege appropriation, which consequently positions AD as a paramount asset for protection within the Zero Trust security strategy.

Consequently, Active Directory (AD) should not merely be considered a target for operational management but must function as a security infrastructure. To achieve this, a variety of security solutions must be implemented concurrently. For instance, a security log analysis system capable of detecting anomalous activities within AD in real-time, the application of a Privileged Access Management (PAM) system that incorporates delegation and approval of administrative rights, and policy audit tools that identify and rectify unnecessary group policies or account settings represent quintessential security technologies. Additionally, it is imperative that regular threat analyses and reinforcement checks specifically targeting AD are conducted.

Active Directory (AD) furnishes foundational data for implementing risk-based authentication policies and granular access control within a zero-trust environment, based on real-time user statuses, device connectivity, and login attempt histories. Consequently, security systems linked with AD must continuously assess user trust and validate permissions based on the information provided by AD. To this end, it is imperative that AD maintains consistently accurate and up-to-date data.

Consequently, Active Directory (AD) transcends its traditional role as a mere user management system, functioning instead as one of the foundational security platforms essential for implementing a zero-trust environment. The degree of sophistication in its operation can significantly influence the overall integrity of the security architecture.

5. Human Resources System (HR System)

HR systems serve as pivotal systems within organizations, managing personnel information such as identity, job roles, departmental affiliations, and employment status for all users. In a zero-trust environment, these systems function as foundational data sources for assessing user trust levels and implementing authorization policies. Whereas traditional security architectures regarded HR systems merely as administrative systems, within the framework of zero trust, their significance is reevaluated as critical interconnected systems essential for user verification and access control.

In this manner, HR systems function as the 'starting point for authorization policies', linking and applying security policies throughout the user lifecycle. They are particularly crucial when changes occur in user attributes such as departmental transfers, job changes, or extended leaves of absence, as these systems must promptly reflect such changes in the interconnected systems. By doing so, it is possible to preemptively block security risks that may arise from the maintenance of unnecessary permissions or the neglect of dormant accounts.

Additionally, HR systems serve as a fundamental basis for the design of RBAC (Role-Based Access Control) and ABAC (Attribute-Based Access Control) policies, which are predicated on user data. These systems are essential for the implementation of the 'principle of least privilege,' a core tenet of Zero Trust security frameworks. Particularly in recent times, data stored in HR systems has been utilized to enhance the accuracy of intelligent access control functions, such as the evaluation of permission appropriateness and the automatic detection of excessive permissions, through the application of machine learning.

Consequently, the HR system should not function as a management system existing independently from the security system, but rather as a pivotal information linkage system that supplies data across the entire zero-trust security framework and regulates user behavior. The accuracy and timeliness of HR information act as critical determinants not only for the precision of user authorization settings but also for the effectiveness of the overall security policy. In this context, the establishment of a systematic integration structure and the continuous assurance of data consistency are paramount.

Each system within the identifiers and identity pillars transcends mere functional units, serving as a substantive means to technically implement a Zero Trust architecture. Systems such as SSO (Single Sign-On), IAM (Identity and Access Management), MFA (Multi-Factor Authentication), AD (Active Directory), and HR systems, while performing independent functions, are interlinked organically. This integration facilitates comprehensive security control throughout the entire process, from user identification to authentication, authorization, and activity monitoring.

Thus, organizations are enabled to implement consistent and precise identity-based access control across diverse environments including physical, virtual, and cloud settings, and to sustain a trust-centric security strategy even amidst a variety of security threat landscapes.

Ultimately, the core principles of Zero Trust, namely 'continuous verification' and 'least privilege', are concretely implemented through such systems, serving as a foundation that elevates an organization's security strategy from theoretical conceptualization to a level that is applicable and operational in real-world environments.

■ Conclusion

In this report, we have meticulously examined the multifaceted dimensions of cybersecurity threats and the corresponding defensive mechanisms that are imperative in safeguarding digital infrastructures. Our analysis delineates the escalating sophistication of cyber-attacks and underscores the necessity for advanced protective strategies to mitigate these risks. It is imperative that organizations continuously evolve their security protocols to stay abreast of the rapidly changing cyber threat landscape. This entails not only the adoption of cutting-edge technologies but also a steadfast commitment to fostering a robust cybersecurity culture within their environments. As we navigate through this digital era, the onus is on both individuals and institutions to fortify their cyber defenses and ensure a secure and resilient cyberspace.
In the Zero Trust architecture, the identifier (Identity) serves as both the inception point of all security strategies and the pivotal axis for assessing and verifying trust in users and entities. Without precise identification and ongoing trust evaluation of various subjects such as users, devices, and service accounts, the core principles of Zero Trust—'continuous verification' and 'least privilege'—risk being reduced to mere formalistic slogans.

The principal systems of identifier pillars, such as SSO, IAM, MFA, AD, and HR systems, are not merely mechanisms performing isolated functions; rather, they constitute an organic and mutually complementary security infrastructure that forms an identifier-based control framework. These systems generate and validate user information, on which they base the allocation of access rights. Furthermore, they detect anomalous activities and adjust policies in real time, thereby distributing the essential security control functions required in a zero-trust environment.

Particularly, the Identifier Pillar serves as a 'hub' that controls and connects the flow of data concerning user identity and permissions, providing a foundation for all other pillars. When the Identifier Pillar is intricately designed and operated, an organization can secure a structural basis that allows for the application of consistent security policies across the entire spectrum of a Zero Trust architecture, including user controls as well as devices, networks, applications, and data. Conversely, if the Identifier Pillar is constructed negligently, it becomes challenging to monitor for abuses of authority, unauthorized access, and insider threats, thereby potentially weakening the continuity of the overall security framework.

Furthermore, the more robustly identifier and identity-based controls operate, the more secure an organization can maintain its status against security incidents. This is significant not merely at the level of preventing incidents but also in that it establishes a foundation for swiftly conducting cause analysis, user history tracking, and forensics in the event of an incident. Such information offers tangible effects across the entirety of security operations, including incident response, recurrence prevention, and policy enhancement.

The identifier pillar is not merely a simple authentication function, but rather a 'foundational pillar' that fundamentally operationalizes the entire zero-trust architecture, and serves as the 'gateway to security strategies'. Organizations should strategically prioritize the construction of this area first, and through a phased approach that expands to other pillars based on this foundation, they can reduce risks to a manageable level and realize a trust-based digital security environment.

References

[1] NIST SP 800-207, "Zero Trust Architecture," August 2020.

[2] Department of Defense, "Zero Trust Overlays," June 2024.

[3] Ministry of Science and ICT/KISA, "Zero Trust Guidelines V1.0", June 2023.

[4] Ministry of Science and ICT/KISA, "Zero Trust Guidelines V2.0," December 2024.

[5] SK Shields, "2025 Security Threat Forecast Report"

[6] SK Shields, "The Genesis of Zero Trust: Perfected with SKZT" - Brochure

[7] SpyCloud, “2025 Identity Exposure Report”

[8] Gatner, "Predicts 2024: AI & Cybersecurity - Turning Disruption Into an Opportunity"

[9] SC Media, "How attackers outsmart MFA in 2025"

[10] Sosafe, "MFA Fatigue Attack"