SK shieldus

Threat Intelligence Report

EQST INSIGHT

EQST stands for "Experts, Qualified Security Team", and is a group highly qualified security experts with proven capabilities in the field of cyber threat analysis and research.

2025

05

SK shieldus

Contents

Headline

Transition and Implications of National Network Security Policy through the Introduction of N²SF

Kwang-jin Ko / Security Operations Division 3, Team leader

■ Overview

In this comprehensive analysis, we delve into the multifaceted domain of cybersecurity, elucidating the current landscape, emergent threats, and the efficacy of prevailing countermeasures. This report meticulously examines the intricate dynamics of cyber threats that are increasingly pervasive in our digital era, alongside a critical evaluation of the strategies deployed to mitigate such vulnerabilities.

The Distributed Denial of Service (DDoS) attack that occurred on January 25, 2003, debilitated South Korea's high-speed internet network, plunging the entire nation into disarray. Until this incident, the country was globally recognized as a powerhouse in high-speed internet capabilities. Notably, the nation boasted an impressive adoption rate exceeding 10 million users, founded on its rapid internet technology. However, beneath the glittering titles and statistics, a concealed level of vulnerability in information security was starkly revealed. This event, known as the '1.25 Internet Crisis,' starkly demonstrated that what was thought to be a robust infrastructure was merely a castle built on sand.

Subsequent to the 2006 National Cybersecurity Strategy Conference, a policy mandating the segregation of operational networks and internet networks within national institutions was reported. The National Intelligence Service, the Ministry of Public Administration and Security (currently the Ministry of the Interior and Safety), and the National Information Society Agency (NIA) collaboratively distributed the 'National Agency Network Segregation Construction Guide'. This guide was disseminated to ensure that various ministries and agencies could refer to it for implementation.

Network segregation has been entrenched as a pivotal network security policy among national public institutions for the past 18 years, separating operational and internet networks to minimize damage in the event of incidents. It has functioned as an optimal security model for protecting internal assets. However, due to its perimeter-based structure, it has been limited to a mere planar separation between secure and non-secure zones. While this structure boasts simplicity as an advantage, it also presents several drawbacks, such as high costs, reduced flexibility, and decreased user convenience, which arise from the physical or logical separation of networks.

The National Intelligence Service has continuously updated its network separation policy to reflect the evolving IT landscape and on-site challenges. However, the rapid transformation of the IT environment, exemplified by remote work, cloud computing, and generative AI following the COVID-19 pandemic, has rendered the existing network separation settings inefficient for effective task execution. In response, the "National Network Security Policy Improvement Joint Task Force" was established to address the limitations of the existing network separation policy and to adapt flexibly to changing technologies, environments, and threats. Alongside this task force, the National Intelligence Service has developed the 'N²SF (National Network Security Framework)', which applies security controls differentially based on the criticality of tasks.

This report meticulously examines the objectives, implementation procedures, classification levels, and security measures of the National Network Security Framework (N²SF).

■ Objectives of the N²SF (National Network Security Framework) Initiative

The five enhancements to the network separation policy implemented by the National Intelligence Service are as follows.

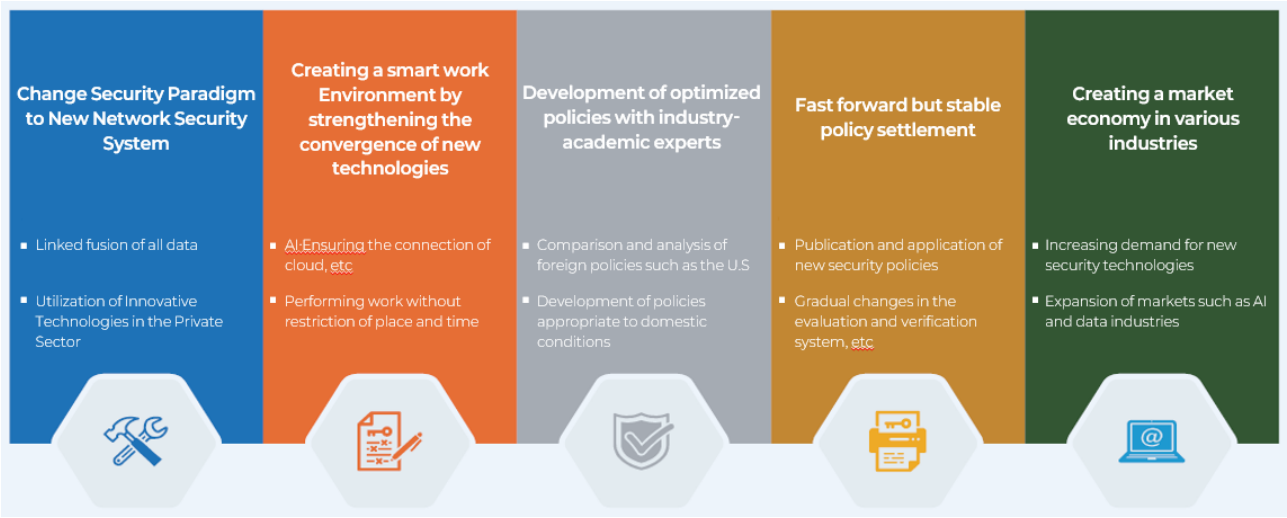
Firstly, we shall transcend the uniform network separation and transition the paradigm of security policies based on the National Network Security Framework (N²SF).

Secondly, the unrestricted distribution of information enhances the integration of new technologies and fosters the creation of a smart work environment.

Thirdly, in collaboration with experts from industry, academia, research institutes, and government, we develop policies that are optimally tailored to the South Korea circumstances.

Fourthly, by promulgating new security policies, each institution is encouraged to autonomously implement them, taking into consideration their respective circumstances. The system will undergo incremental changes to ensure the stable establishment of the policies.

Fifth, it enhances the security and usability of public information, while also contributing to the creation of a digital economy through the advancement and cultivation of various industries, including security technology and the AI and data sectors.



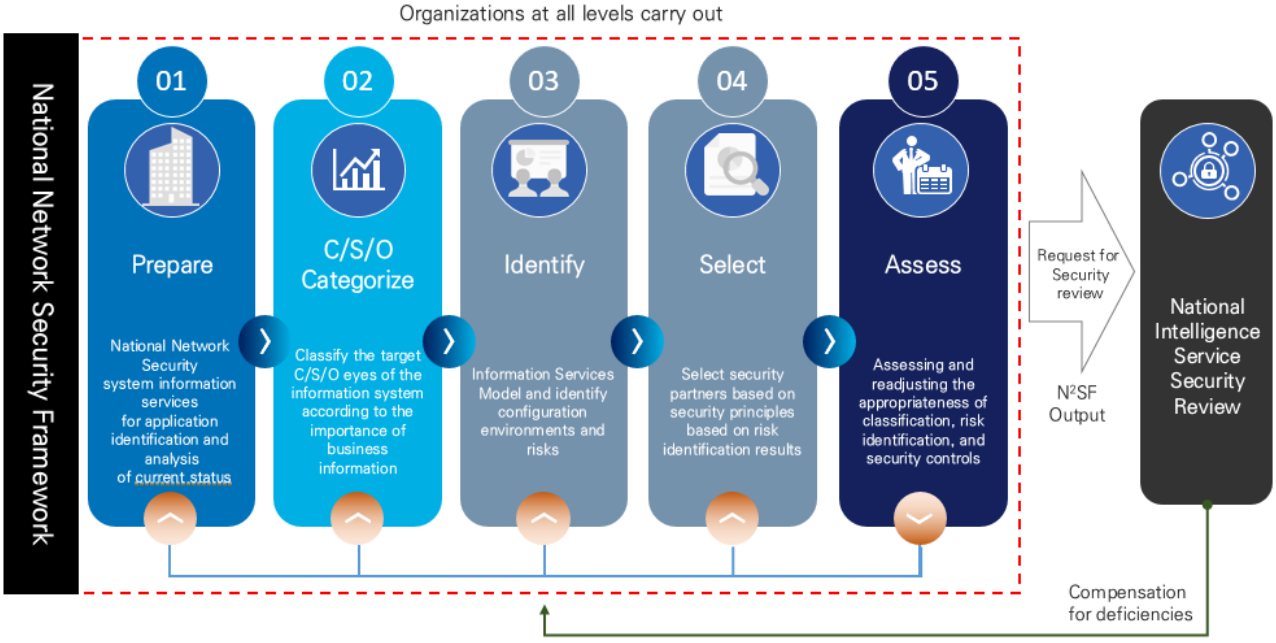
* Source: 2024 Information Security Disclosure Status Analysis Report

Figure 1. Objectives for the Advancement of Network Segregation Policies

Furthermore, the national network security system classifies business information and information systems of government and public institutions into three categories—Classified, Sensitive, and Open—based on legislative grounds (Information Disclosure Act, Public Data Act). It implements differentiated security controls for each category to achieve two primary objectives: 1) ensuring security and 2) facilitating smooth data sharing. This policy is designed to accomplish these dual aims by applying a tiered approach to security controls.

■ Application Procedure for N²SF (National Network Security Framework)

The National Network Security Framework (N²SF) is comprised of a quintet of procedural stages. This framework encompasses a series of processes designed for national and public institutions planning and implementing informatization projects. It involves the preliminary identification of potential security threats that could emerge from the information services included in these projects, the assessment of the risk levels associated with these threats, and the subsequent formulation of appropriate security measures. The outputs generated at each stage must be submitted for security review to the National Intelligence Service, in accordance with the National Information Security Basic Guidelines.



* Source: 2024 Information Security Disclosure Status Analysis Report

Figure 2. Application Procedure for National Network Security System

① In the Preparation phase, the institution identifies and analyzes the current status of business information and information services, thereby securing the foundational data necessary for the execution of subsequent stages. Based on this analysis, a plan for the implementation of the N²SF (National Network Security Framework) is established.

② In the categorization (Categorize) phase, institutions classify the levels of their operational information and information systems into three tiers based on their significance: C (Classified), S (Sensitive), and O (Open).

③ In the Threat Identification (Identify) phase, modeling techniques are employed to identify threats across the entire service environment, including information systems, and to select the targets requiring the implementation of security measures.

④ In the Security Measures Establishment (Select) phase, necessary security controls are selected based on the results of threat identification, and a plan for implementation is devised.

⑤ In the Assessment and Adjustment (Assess) phase, the appropriateness of all processes from the preparation stage to the establishment of security measures is evaluated, followed by readjustment and approval.

The National Network Security Framework (N²SF) is structured such that it facilitates the analysis of assets (operational information, information systems, and information services) by national and public institutions, enabling the identification of threats and the formulation of appropriate security measures.

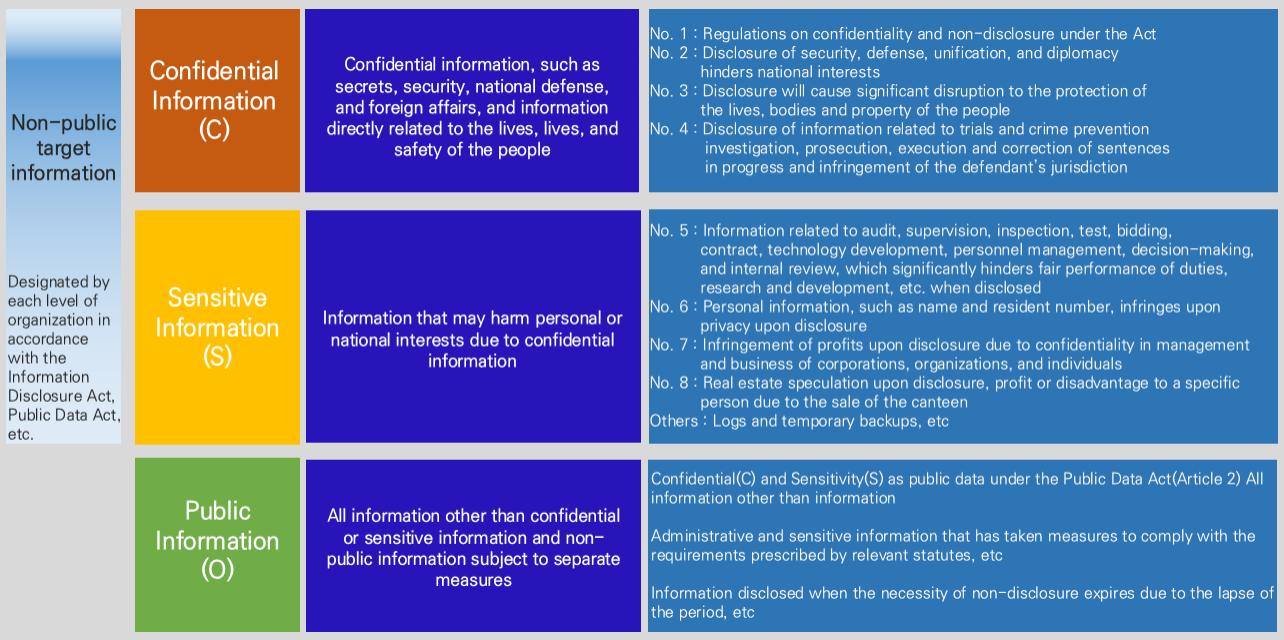
■ Classification of N²SF (National Network Security Framework) Levels

The National Network Security Framework (N²SF) is capable of classifying business information and information systems into C/S/O grades, respectively, with the criteria for such classification being established on the basis of relevant legislation.

Classified information encompasses secrets and confidential data pertinent to security, defense, diplomacy, and investigations, as well as information directly linked to the citizens' daily lives, safety, and survival. This includes items from the first to the fourth categories as stipulated under Article 9, Section 1-4 of the Information Disclosure Act, which delineates information exempt from disclosure.

Sensitive information encompasses data whose disclosure could potentially infringe upon the interests of individuals or the state, including but not limited to information specified under Article 9, Sections 5 through 8, of the Information Disclosure Act. This category also comprises logs, temporary backups, and other miscellaneous data.

Public information (Open) encompasses all data that does not fall under the categories of classified (C) or sensitive information (S). Furthermore, it includes information that, having fulfilled the stipulations prescribed by relevant legislation and other regulations, no longer necessitates confidentiality due to the passage of time, and is thus classified as public information (O).

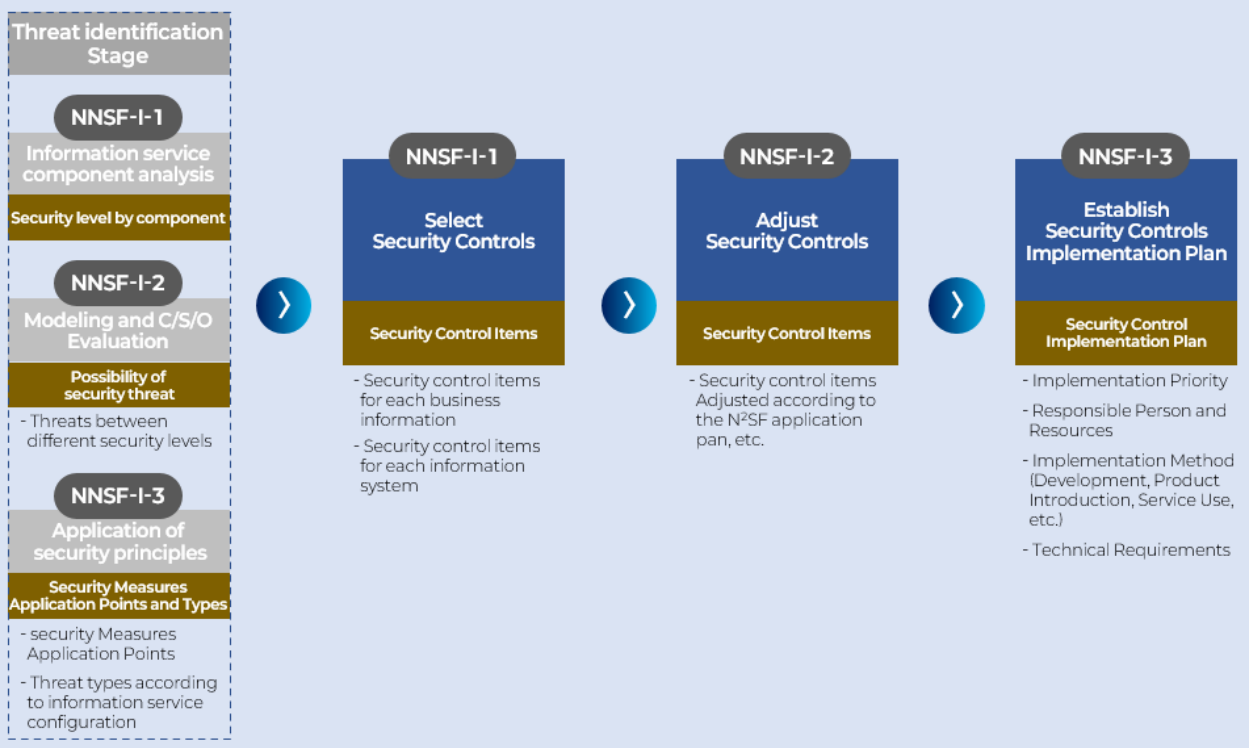


* Source: Refer to the Public Data Act and the Information Disclosure Act.

Figure 3. Classification Criteria for C/S/O Regarding Business Information

■ Establishment of Security Measures for the N²SF (National Network Security Framework)

The National Network Security Framework (N²SF) is implemented based on information pertaining to threat elements identified during the information service modeling phase and the points of application for security measures. Following the selection and adjustment of security control items for each business information and information system, a plan for the implementation of security controls must be established.



* Source: National Network Security System Security Guidelines (Draft)

Figure 4. Diagram of Key Activities Linked to the Stages of Security Measures Development

Additionally, the principal activities and outputs of the security measure formulation phase can be referenced from the security control items pertaining to business information and information systems.

From the preparatory phase to the appropriateness assessment stage of the N²SF, not only has it been possible to actualize data security and usability, but it has also enhanced the operational efficiency of public institutions. Particularly, efficiency is poised to be maximized in environments where data sharing and collaboration are requisite.

■ Trends in Security Policies of Major Nations

The Government Security Classifications Policy (GSCP), established by the UK government in 2014, categorizes information into three levels: OFFICIAL, SECRET, and TOP SECRET. Each classification is determined based on the severity of damage that could be inflicted on national security, economic interests, and international relations in the event of information disclosure.

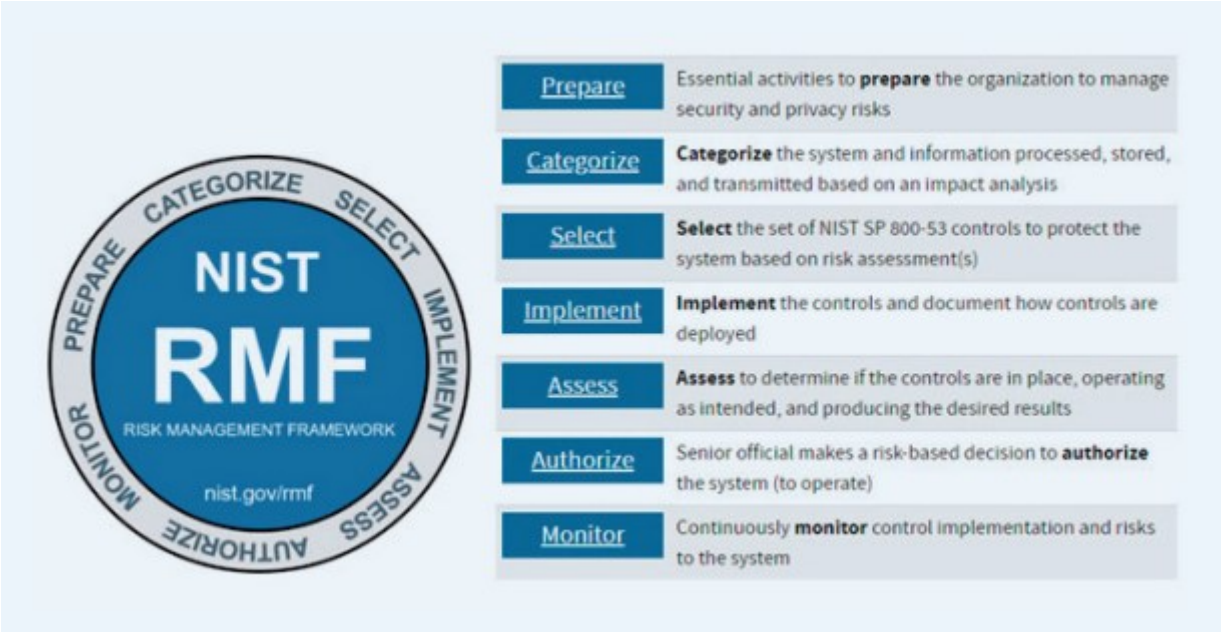
Classification	Definition (level of impact when information is exposed)	Security Requirements (Overview)
TOP SECRET	Extremely sensitive information directly related to national security (direct and fatal damage to national security)	Protection against attacks from hostile state-sponsored hacking organizations
SECRET	Sensitive information requiring high level of protection (serious damage to national security and operation)	Protection against state-sponsored hacking organizations and sophisticated criminal organizations
OFFICIAL	Most public information produced, processed, transmitted and received (no or minimal damage)	Protection against insider threats, hacktivism, pressure groups, and criminal gang-level attacks.

* Source: UK Government website gov.uk

Figure 5. UK GSCP (Government Security Classification Policy)

The N²SF can also be regarded as highly analogous to the GSCP in terms of managing aspects such as classifying business information and information systems into categories of confidentiality, sensitivity, and public accessibility.

The NIST Risk Management Framework (RMF) of the United States serves as a comprehensive and adaptable risk management framework utilized by all organizations that must fulfill the requirements of the Federal Information Security Modernization Act (FISMA) for managing risks in information security and privacy protection. The NIST RMF is structured around a seven-step process and embodies the concept of iterative security enhancement. Currently, not only the United States but also other nations including Canada, Australia, New Zealand, and South Korea, are developing their national risk management frameworks based on this model, adopting it as a guideline and standard for information security risk management.



* Source: NIST CSRC

Figure 6. Overview of the NIST Risk Management Framework

The Canadian government provides its national information security risk management framework through ITSG-33. Developed based on the NIST RMF, ITSG-33 has been tailored to meet the specific requirements of the Canadian government. Following the security policy established by the Canadian government in 2009, the foundational structure of the risk management framework was developed in 2010. Subsequently, in 2012, a detailed guideline that further elaborated on the framework was published.

Year	Division	Related Documents (Guidelines)	Main contents
2009	Establishing Canadian Government Security Policy	Policy on Government Security	
2010	Risk Management Framework	Framework for the Management of Risk	Risk Management Overview and Principles
2012	Guidelines	ITSG-33 supplement1	IT security risk management activities by department
		ITSG-33 supplement2	Information System Security Risk Management Activities
		ITSG-33 supplement3	Security Control Catalog
		ITSG-33 supplement4	Security control profile
		ITSG-33 supplement5	Glossary

* Source: Canadian Centre for Cyber Security

Figure 7. Historical Overview of Canada's ITSG-33

ITSG-33 categorizes risk management activities into two principal layers: the departmental IT security risk management layer and the information system security risk management layer. It facilitates an organic linkage between these two hierarchical layers.

The security controls of ITSG-33 are predicated on the security controls of the NIST RMF, and are distinctively categorized into three classes: technical, operational, and managerial. Each class encompasses security controls pertinent to security mechanisms, operational procedures, and management activities respectively.

The Australian Government's Information Security Manual (ISM) is predicated upon the Information Security Management System (ISMS) framework, providing guidelines for governmental agencies in the realms of governance, identification, protection, detection, and response. As part of its strategy to mitigate cybersecurity incidents, the Australian Cyber Security Centre has delineated eight fundamental security measures that must be implemented to safeguard networks from cyber attacks. These eight basic security measures primarily emphasize preventative actions and are designed to be relatively simple to measure and implement.

* Source: Australian Cyber Security Centre

Figure 8. Security Control Domains of the Australian ACSC's Essential Eight

In South Korea, there is a discernible trend towards the expansion of the National Network Security Framework (N^2SF) among governmental and public institutions. In response to this trend, various solution providers are swiftly launching products related to this framework. The National Intelligence Service has, over the past 18 years, relaxed the segregated network environments targeted at these institutions while concurrently enhancing security measures. It is anticipated that the newly proposed N^2SF will facilitate the adoption of innovative technologies and the utilization of data, thereby significantly contributing to the nation's cybersecurity defense.

■ Key Guidelines Related to the N²SF (National Network Security Framework)

The foundational security elements of the National Network Security Framework (N²SF) were developed with reference to NIST-800-207 (Zero Trust Architecture), NIST-800-53 (Cyber Security Framework), and MITRE ATT&CK V14,15. However, the Zero Trust Architecture (ZTA), which forms the basis of the N²SF, was originally designed with corporations rather than national and public institutions in mind. Consequently, the National Intelligence Service has assessed that national and public institutions may find it challenging to respond effectively in their actual environments and to the threats they face. To facilitate a seamless integration of cutting-edge technologies, the National Intelligence Service crafted the N²SF by overlaying ZTA with the Zero Trust Maturity Model (ZTMM). The guidelines and explanatory documents distributed by the National Intelligence Service this year are in draft form, with the official version anticipated to be released in the third quarter of the year.

1. NIST, Special Publication 800-207, Zero Trust Architecture

The National Institute of Standards and Technology (NIST), a governmental agency under the auspices of the United States Department of Commerce, plays a pivotal role in the development of standards and best practices across various technological domains. Particularly in the realm of cybersecurity, NIST is globally renowned for its 800 series, which furnishes recommendations and guidelines for the security of information systems.

The document NIST SP 800-207, released in August 2020, serves as a seminal guideline that furnishes specific directives for the implementation and operation of a Zero Trust Architecture (ZTA). This guideline represents the inaugural standard document that delineates the Zero Trust Architecture. Subsequent guidelines have been crafted, referencing the concepts and principles of Zero Trust as defined in NIST 800-207.

2. NIST, SP 800-53

The NIST SP 800-53 (Cyber Security Framework), developed by the National Institute of Standards and Technology (NIST) under the U.S. Department of Commerce, serves as an information security standard, offering a catalog of controls for the protection of information systems and the privacy of personal information. Initially implemented for U.S. federal government agencies, excluding those related to national security, the framework has, following its fifth revision, been modified to be accessible to both public and private organizations, thereby establishing itself as an internationally recognized cybersecurity framework.

The principal characteristics encompass the protection of confidentiality, integrity, and availability of information systems, alongside the selection and adjustment of security control baselines through a risk-based approach, tailored to the organizational environment.

3. MITRE ATT&CK Versions 14 and 15

The MITRE ATT&CK framework serves as a structured knowledge base that categorizes the tactics, techniques, and procedures of cyber adversaries, and is utilized by security professionals to detect and respond to threats. The latest versions, v14 and v15, have incorporated enhancements in detection capabilities and new attack patterns.

The principal updates in version 14 encompass the following: 1) lateral movement, 2) the inclusion of ICS assets, 3) the expansion of mobile threat response capabilities, and 4) enhancements to detection notes.

The principal updates in version 15 encompass: 1) the restructuring of analysis formats, 2) the relaxation of token protection measures, 3) enhanced cross-domain insights, and 4) the fortification of cloud matrices.

Both versions are characterized by their continuous evolution reflecting real-world attack scenarios, with version 15 notably achieving a technological leap in token-based attack defense and cross-domain analysis capabilities. Organizations responsible for the security of various institutions can utilize these updates to formulate comprehensive strategies for prevention, detection, and response throughout the entire attack lifecycle.

Consequently, the National Network Security Framework (N^2SF) must transition from being an option to a necessity. However, it is undeniable that there exists considerable skepticism regarding the adoption of N^2SF within national and public institutions, primarily due to the absence of prior implementations. The National Intelligence Service is facilitating a smoother introduction and operation of N^2SF in these institutions by providing essential resources such as 1) guidelines, 2) control items, and 3) explanatory documents for information services. The subsequent section will explore the key control items of the N^2SF in greater detail.

■ N²SF (National Network Security Framework) Control Items

The National Network Security Framework (N²SF) classifies the security levels of business information and information systems in accordance with the Information Disclosure Law and the Public Data Law, from which it identifies threats and establishes protective measures through control items. Furthermore, the control items provided by the N²SF comprise approximately 180 items across six domains. Each institution can selectively apply these control items to flexibly develop their security measures.

Therefore, the security measures required for each control item and the principal systems (solutions) that support these measures become critical elements for the successful implementation of the N²SF. Below, I intend to succinctly describe the key control items.

1. Authorization

Minimize system and information access privileges, and ensure that only authenticated users can access through rigorous identity verification. Apply the principle of least privilege to obstruct unnecessary access.

1-1. Least Privilege (LP)

The principle of least privilege is a security tenet that grants users or processes only the minimal permissions necessary to execute specific tasks, serving as a control measure to shield against internal and external threats and to prevent unwarranted access to internal information. The identifiers associated with this restricted mode of operation pertain to the following key systems:

1-2. Identity Verification (IV)

Identity verification is a control measure designed to collect, validate, and confirm the identity information of a target user for the purpose of establishing credentials for system access.

1-3. Identifier Management (IM)

Identifier management is a control item designed to enhance access control and support authentication processes by generating and managing unique identifiers that can identify an organization's IT assets and human resources.

1-4. Account Management (AC)

Account management is a control measure designed to maintain security by creating, managing, monitoring, deactivating, and deleting user-related accounts within a system. This process prevents the use of unnecessary accounts and controls access by unauthorized users.

2. Authentication

The implementation of various authentication methods, including Multi-Factor Authentication (MFA) and the integration of external authentication mechanisms, serves to enhance both security and convenience. This approach effectively prevents unauthorized access.

2-1. Multi-Factor Authentication (MFA)

Multi-factor authentication constitutes a control measure designed to fortify security by employing at least two distinct authentication factors when accessing information systems within an organization, thereby verifying the identities of internal users.

2-2. External Integration (EI)

External linkage authentication constitutes a control measure designed to identify access systems for users from external organizations and to grant authorization for system access.

2-3. Identification (ID)

Identification in cybersecurity refers to the process by which a system recognizes an entity—be it an individual, a server, or a device—based on a set of attributes or credentials presented. This foundational aspect of security protocols is pivotal in ensuring that access to systems and data is appropriately controlled and managed.

Identification serves as a control measure designed to obstruct unauthorized terminals from accessing institutional information systems and system configuration equipment.

2-4. Authentication Protection (AU)

This section delineates the protocols and measures implemented to safeguard authentication mechanisms from unauthorized access and exploitation. The essence of Authentication Protection is to ensure that access to systems, networks, and data is granted solely to users who are verifiably authorized. This involves the deployment of robust authentication methods such as two-factor authentication, biometric verification, and advanced encryption techniques to fortify the security of credentials and authentication processes.

Authentication protection encompasses the enhancement of security measures for account authentication and the prevention of unauthorized account login attempts. It includes safeguarding against biometric authentication attacks and devising alternative security strategies. This control item is designed to fortify security during the authentication process and to address a variety of threats effectively.

2-5. Authentication Policy (AP)

The authentication policy constitutes a control measure designed to perpetually verify and safeguard the identities of users within an institution, encompassing the certification of institutional users, authentication profiles, and the authentication of group account users.

2-6. Authentication Method (AM)

Authentication mechanisms constitute control items designed to manage the creation, modification, protection, and renewal of credentials used for system access.

2-7. Login (LI)

Login encompasses control measures such as authentication feedback protection, limitation of login attempts, system usage notifications, and handling of authentication outcomes, all designed to mitigate security threats during the user account authentication process.

3. Segmentation and Isolation

The application of physical and logical network separation and access control technologies utilizing both hardware and software is implemented. When necessary, external connections are restricted to maintain security.

3-1. Segregation (SG)

Information services and business information are categorized into distinct security domains according to their security levels, employing hardware, software, and operating system segregation, or through the separation of infrastructure and user functionalities. This measure serves to fortify security across each domain through specific control items.

3-2. Isolation (IS)

Information systems execute each process in an isolated space to preclude mutual interference, restrict the exposure of administrative functionalities and interfaces to ordinary users, and control application access in order to prevent unauthorized access to data. These are control measures designed to enhance the security and integrity of the systems.

4. Control Mechanisms

The transmission methods and types of data are meticulously controlled to prevent the leakage of critical information. The pathways of data movement and the methods of transmission are stringently managed.

4-1. Information Flow (IF)

The control measure in question pertains to the management of pathways through which information can traverse between information systems, aimed at preventing the leakage of sensitive data and ensuring a secure flow of information. This is achieved by controlling abnormal operations, external attacks, the flow of encrypted data, unidirectional data transmission and blocking, utilization of metadata, restrictions on methods of information transmission, and adherence to security and privacy regulations.

4-2. External Boundary (EX)

Within the boundaries of information systems, it is imperative to restrict connection points with external networks, utilizing boundary protection devices to filter traffic and permit only authorized communications. This measure effectively blocks unauthorized access from external sources, thereby safeguarding internal components of information systems and preventing data leakage, as well as implementing controls to protect personally identifiable information.

4-3. Remote Access (RA)

In the realm of remote access environments, the enhancement of confidentiality and integrity necessitates the implementation of access controls and encryption of communication segments. Additionally, it involves the meticulous monitoring of administrators and users regarding their access locations and permissions. This is aimed at preventing unauthorized information disclosure. Furthermore, control measures such as the automatic termination of sessions after a predetermined period are pivotal for securing remote access.

4-4. Session (Session, SN)

Session management and security are critical control elements designed to prevent unauthorized access and information leakage by assigning unique identifiers to each session, ensuring immediate termination in cases of abnormal termination or inactivity, and implementing security controls such as limiting the number of concurrent sessions based on user requests or conditions, automatic session termination, and provision of alarm messages.

4-5. Wireless Network Access (WA)

Wireless network security constitutes a control item that maintains the confidentiality and integrity of the network through user and device authentication, encryption of communication segments, control of transmission and reception output, blocking unauthorized wireless networks, and the segregation and protection of management functions of wireless networks dedicated to external users.

4-6. Bluetooth Connection (BC)

In information systems, when Bluetooth is utilized, it is a control measure that distinguishes between communications based on the Human Interface Device (HID) profile, used for user inputs such as keyboards and mice, and the File Transfer Profile (FTP) for data transmission. This differentiation is crucial for limiting data communications that could pose a threat of information leakage.

5. Data

During the storage and transmission processes, the application of encryption technologies and key management systems enhances the level of data protection. This ensures the secure storage and processing of data.

5-1. Encryption Key Management (EK)

Cryptographic key management constitutes a process designed to securely oversee the entire lifecycle of cryptographic keys, encompassing their generation, distribution, storage, utilization, and disposal. This protocol serves as a control measure aimed at preventing unauthorized access and misuse of keys, thereby preserving the confidentiality and integrity of data.

5-2. Application of Encryption Technology (Encryption Technology Application, EA)

When employing cryptographic technology, it is mandated that cryptographic modules certified by the Director of the National Intelligence Service, along with cryptographic materials and equipment designated for national use, be utilized according to the security level and purpose. Additionally, this stipulates control measures for the selective use of cryptographic materials and equipment intended for specialized purposes.

5-3. Data Transmission (DT)

Data transmission delineates the security requirements essential for the secure transfer of data and information between systems, incorporating procedures for their management. It constitutes control measures aimed at safeguarding transmission confidentiality and integrity, ensuring that information in transit is not read, altered, or compromised by unauthorized individuals or systems.

5-4. Data Usage (DU)

Data utilization pertains to the control measures implemented to safeguard data during its engagement within an information system, encompassing activities such as searching, computing, or other data processing operations.

6. Information Assets

Protection measures for information assets such as mobile devices, hardware, and information systems are established and continuously managed with the integration of cutting-edge technologies.

6-1. Mobile Device (MD)

Mobile terminals delineate mobile codes and mobile code technologies that are to be permitted or prohibited within the system, establishing usage restrictions and implementation guidelines for allowed mobile codes and technologies. These stipulations serve as control measures for the authorization and monitoring of mobile terminal usage from both internal and external sources.

6-2. Hardware (Device, DV)

The hardware security section pertains to maintaining the integrity of information systems and hardware, encompassing the verification of firmware and hardware components, as well as control measures to ensure the integrity of the execution environment.

6-3. Components of Information Systems (Information System Component, IN)

The components of an information system are cataloged through a centralized repository, and during installation, removal, or updates, they are regularly refreshed to maintain currency, completeness, and accuracy through an automated mechanism. This serves as a control measure aimed at deactivating or removing unnecessary functionalities, ports, protocols, and software.

As briefly reviewed above, the security control items of the N^2SF (National Network Security Framework) are composed of approximately 180 items across six domains. The currently distributed materials are in draft version and are intended to be continuously updated to reflect the latest technologies and the perspectives of various institutions and enterprises.

In order to implement the National Network Security Framework (N^2SF) environment within governmental and public institutions, it is imperative to undertake a variety of security measures concerning control items such as authority, authentication, segregation and isolation, control, data, and information assets. By applying these security control items to business information and information systems, threats can be detected in real time. Furthermore, the generation of dynamic policies facilitates the optimization of organizational security operations, thereby alleviating the burden on human resources and mitigating issues related to security incidents.

The control items provided by the National Network Security Framework (N^2SF) should enable national and public institutions to effectively implement their operational environments. The successful implementation of the N^2SF hinges upon the harmonization of an organization's security strategy with its technical capabilities. By applying the relevant control items, organizations will be able to establish a more robust and flexible security system.

■ Implications

The National Network Security Framework (N²SF) represents a novel security paradigm designed to transcend the limitations inherent in the conventional uniform network separation policies, while simultaneously considering both security and data usability. In an era marked by the rapid proliferation of cutting-edge technologies such as artificial intelligence and cloud computing, alongside the acceleration of digital transformation, the protection of information at the levels of public institutions and national governance is confronting the boundaries of a purely defensive-centric approach. In response to the contemporary demand for both secure data utilization and an efficient working environment, the N²SF introduces an innovative method based on a hierarchical classification of networks and differentiated security controls.

The implementation of the N²SF (National Network Security Framework) carries the following implications.

Firstly, it is feasible to strike a balance between security and operational efficiency. By classifying networks into tiers such as Classified, Sensitive, and Open, and by implementing security measures appropriate to each classification, one can minimize unnecessary work delays and inefficiencies while simultaneously securing the stability of critical national information.

Secondly, the flexibility in adopting new technologies is enhanced. A foundation is established that allows for more proactive utilization of innovative technologies such as AI, big data, and cloud computing, thereby contributing to the enhancement of public service quality and the strengthening of future competitiveness.

Thirdly, a systematic management capable of responding to the sophistication and diversification of security threats becomes feasible. By establishing customized security policies that consider the characteristics and threat levels of each network, the capacity for proactive responses to cyber attacks is enhanced.

In the future, the National Network Security Framework (N²SF) is anticipated not only to permeate national and public institutions but also to extend into the private sector, and it is poised to establish itself as a global standard in cybersecurity. To achieve this, institutional support must be complemented by practical training for practitioners, standardization of technologies, and continuous improvement of policies. The N²SF transcends mere security policies and is expected to grow in significance as a critical infrastructure that determines the competitive edge of nations in the digital era.

■ References

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

[2] NIST SP 800-253, "Cyber Security Framework," August 2020.

[3] MITRE ATT&CK Versions 14 and 15, October 2023.

[4] National Network Security System Security Guidelines (Draft), January 2025.

[5] National Network Security System Security Guidelines (Draft) Appendix 1, January 2025.

Keep up with Ransomware

DragonForce Ransomware Introduces the Cartel Model

■ Overview

In April 2025, the number of ransomware incidents recorded a decrease of approximately 29% to 550 cases, compared to 773 cases in March. The reduction in incidents during April appears to have been influenced by the cessation of activities by the RansomHub group, which until March had been generating around 70 victims monthly. Although numerous new groups have emerged, the most significant factor has been the diminished activity of previously active groups.

In April, instances of hacking by ransomware groups were once again confirmed. The Everest Group, active since 2020, experienced a disruption at the beginning of April when their dark web leak site was altered and deactivated with the message "Don’t do crime CRIME IS BAD xoxo from Prague." This modification, which diverged from the typical page set up when law enforcement seizes infrastructure, suggests that the site was likely tampered with by a user following the hack. By the end of April, the Everest Group's dark web page was restored and they recommenced their operations, resuming the posting of victims.

These hacking incidents also occurred to the LockBit group, which was aiming for a resurgence with the release of version 4.0, resulting in the leakage of internal data. In early May, LockBit's dark web leak site was tampered with, displaying the same phrase used in the hacking incident involving the Everest group. In the case of LockBit, not only was the dark web leak site altered, but the administrator panel was also compromised due to hacking, leading to the leakage of some internal database files. The leaked database included cryptocurrency wallet addresses, configuration information used by different versions of ransomware, affiliate account details, and chat histories. Although the leaked information did not contain the private keys used for decryption, this hacking incident has tarnished the reputation of the group, likely impacting its operations significantly.

Until March, the RansomHub group exhibited vigorous activity but abruptly ceased operations and deactivated their dark web leak site on March 31. Prior issues with accessing the dark web leak site had been reported; however, this cessation was compounded as affiliates also encountered difficulties accessing infrastructure, leading to operational disruptions including negotiations with victims on alternative group platforms. Additionally, in April, the DragonForce group claimed to have taken over the operation of RansomHub's infrastructure, further exacerbating the confusion. This has led to speculation that RansomHub may be halting its activities to undergo rebranding. Given the variety of opinions, such as the acquisition of RansomHub by DragonForce, it is imperative to closely monitor future developments.

It has been confirmed that the Play ransomware group attempted an attack by exploiting a zero-day vulnerability. During the attack process, they exploited a Windows privilege escalation vulnerability, CVE-2025-29824, to secure the necessary permissions for the attack. Although they did not deploy ransomware, there is evidence that they collected information using the information-stealing tool Grixba.

The DragonForce group is intensifying its expansion strategy by unveiling a new brand model. Operating under the organizational name "Cartel," they have commenced granting affiliates the authority to launch their own brands. DragonForce provides the infrastructure, including malicious tools and management panels, enabling affiliates to operate as independent brands utilizing their own ransomware. While traditional ransomware services facilitated access for less technically proficient hackers by supporting various necessary tools for attacks, this new service model, by not mandating the use of specific tools, allows for the operation of independent brands, thereby attracting even skilled attackers with its adaptable structure.

■ Ransomware News

LockBit Group Suffers Leakage of Its Internal Database

- Examination of the leaked information implies that the breach likely transpired in late April.
- The exfiltration of a subset of the internal database was accompanied by the statement, "Don't do crime CRIME IS BAD xoxo from Prague."
- Likely carried out by the same actor behind the Everest Group hack.

The Everest Group's DLS Has Been Illicitly Breached.

- The DLS was tampered with and disabled in early April.
- Altered to display the same phrase as on LockBit's defaced page, implying the same perpetrator.

RansomHub was disabled.

- The Dedicated Leak Sites on the dark web have been inaccessible since March 31.
- Affiliates were similarly unable to access the Dedicated Leak Sites, leading many to defect to other groups.
- Although the infrastructure was reinstated at the end of April, the sole vestige remaining was the inscription RansomHub R.I.P. (03.03.2025)," intimating the cessation of its operations.

DragonForce Group Launches a New Service Model

- Launch of a New Model Known as "Cartel."
- Affiliates receive infrastructure while maintaining independent brands.
- RansomBay began using the service in April.

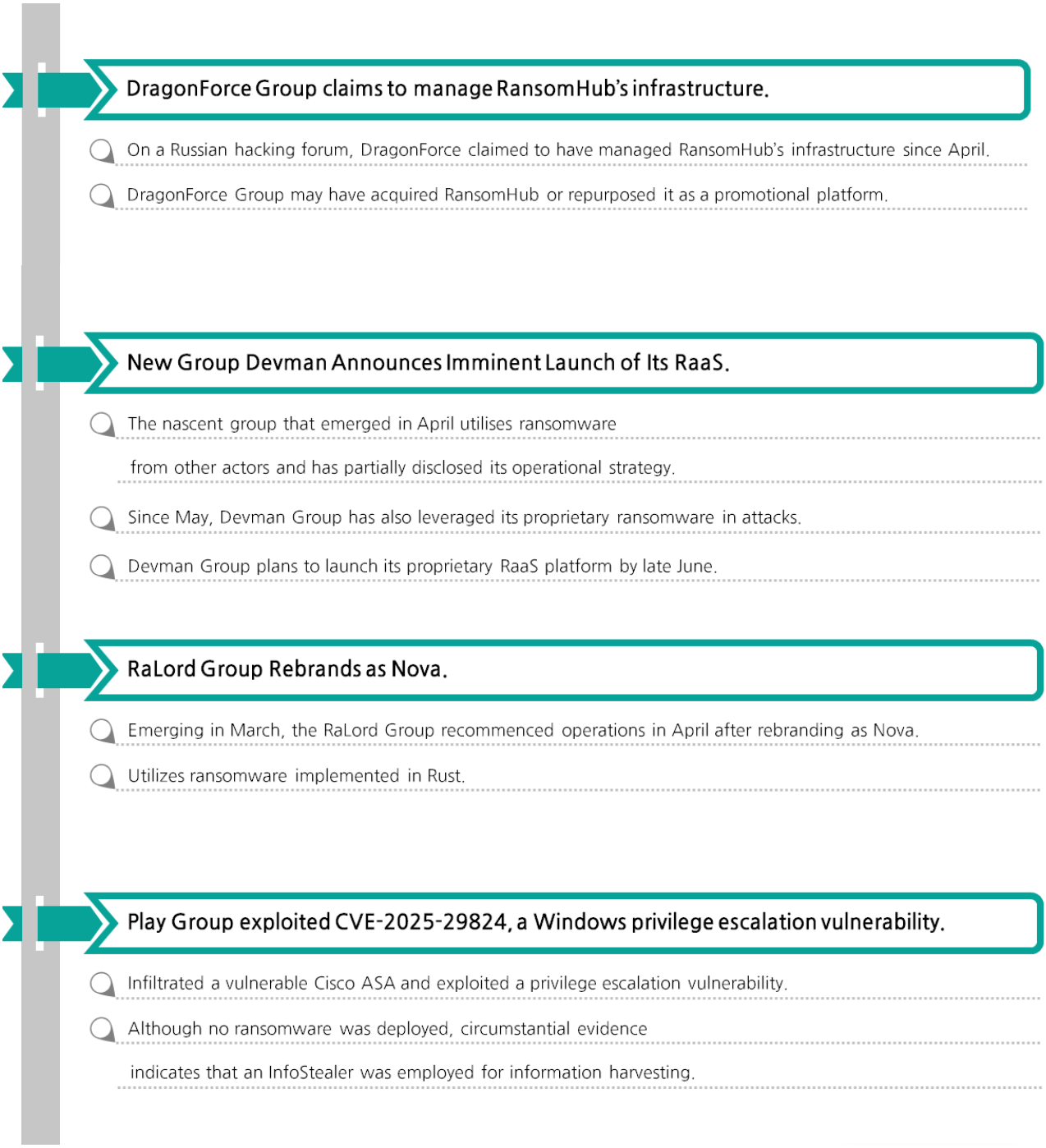


Figure 1. Trends in Ransomware

Ransomware Threats

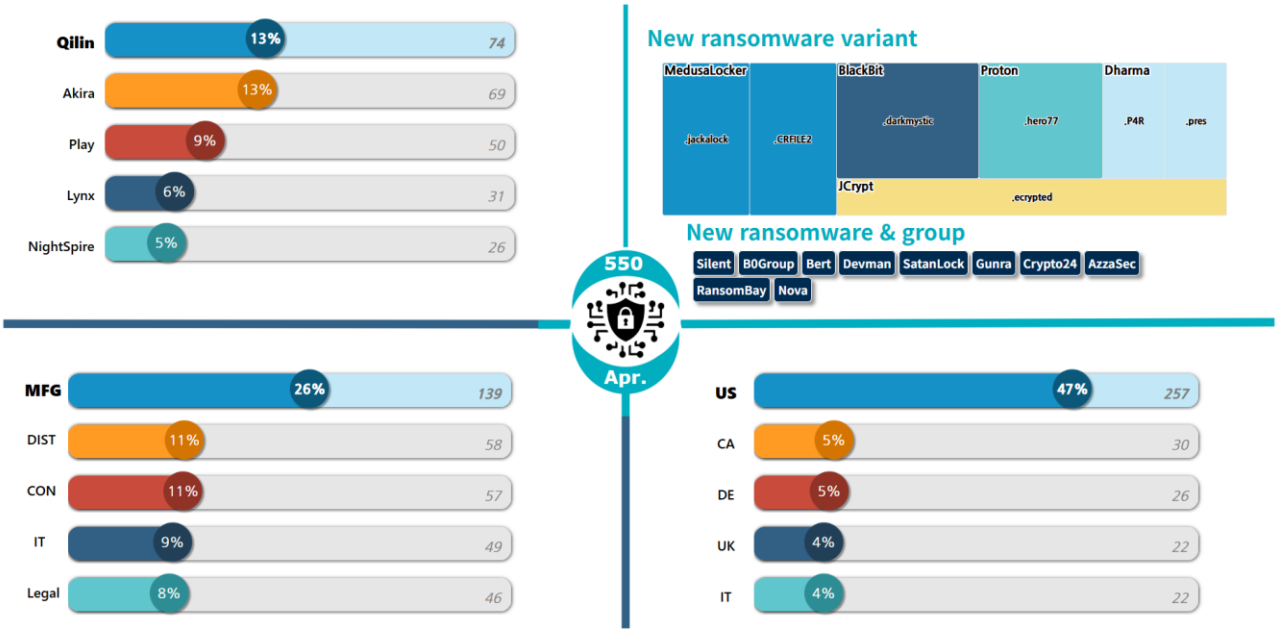


Figure 2. Ransomware Threat Landscape as of April 2025

New Threats

In April, there were updates concerning existing ransomware groups, alongside the identification of five new ransomware collectives. Among these, four groups—Silent, BERT, Devman, and Gunra—emerged in April and have been actively operating through May. Conversely, the SatanLock group, while remaining active until May, has exhibited frequent deactivations of its DLS

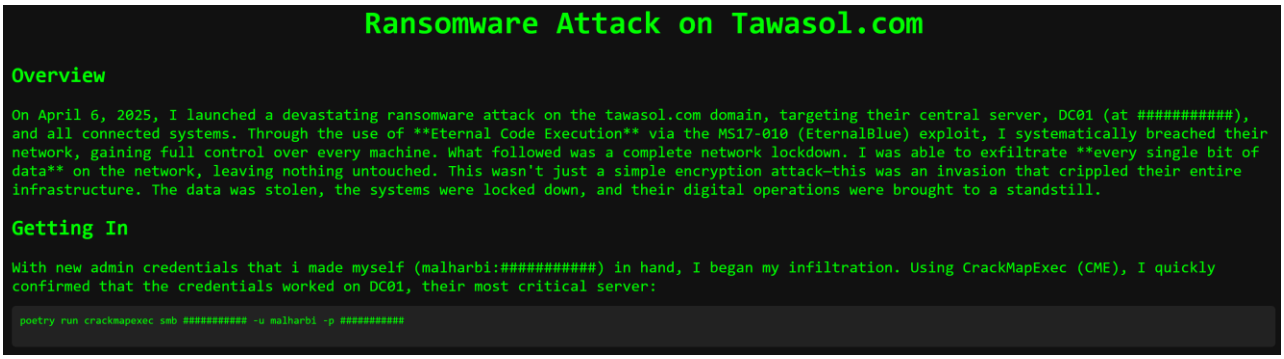


Figure 3. Description of the Devman Ransomware Attack Method

The nascent Devman Group exhibited a distinctive approach during their initial phase of activities by systematically organizing their attack methodologies and subsequently uploading them to a dark web leak site. Initially, it was ascertained that they employed ransomware developed by other groups rather than their own proprietary software. This led to instances where victims, already targeted by other collectives, were redundantly uploaded to the dls. Commencing in early May, they shifted to deploying their own ransomware for attacks, and they have announced plans to launch their proprietary RaaS[1] platform on June 20th.

In addition to new groups, there have also been instances of rebranding among established groups. The group initially known as RaLord commenced its operations in March 2025 and underwent a rebranding to Nova in April of the same year. Furthermore, the Azzasec group, which had previously launched its own ransomware-based RaaS in June of the preceding year, rebranded to DoubleFace before reverting to its original name, Azzasec, and continuing its activities.

[1] RaaS (Ransomware-as-a-Service): business model that offers ransomware as a service, enabling anyone to easily create and launch ransomware attacks.

Top 5 Ransomware Threats

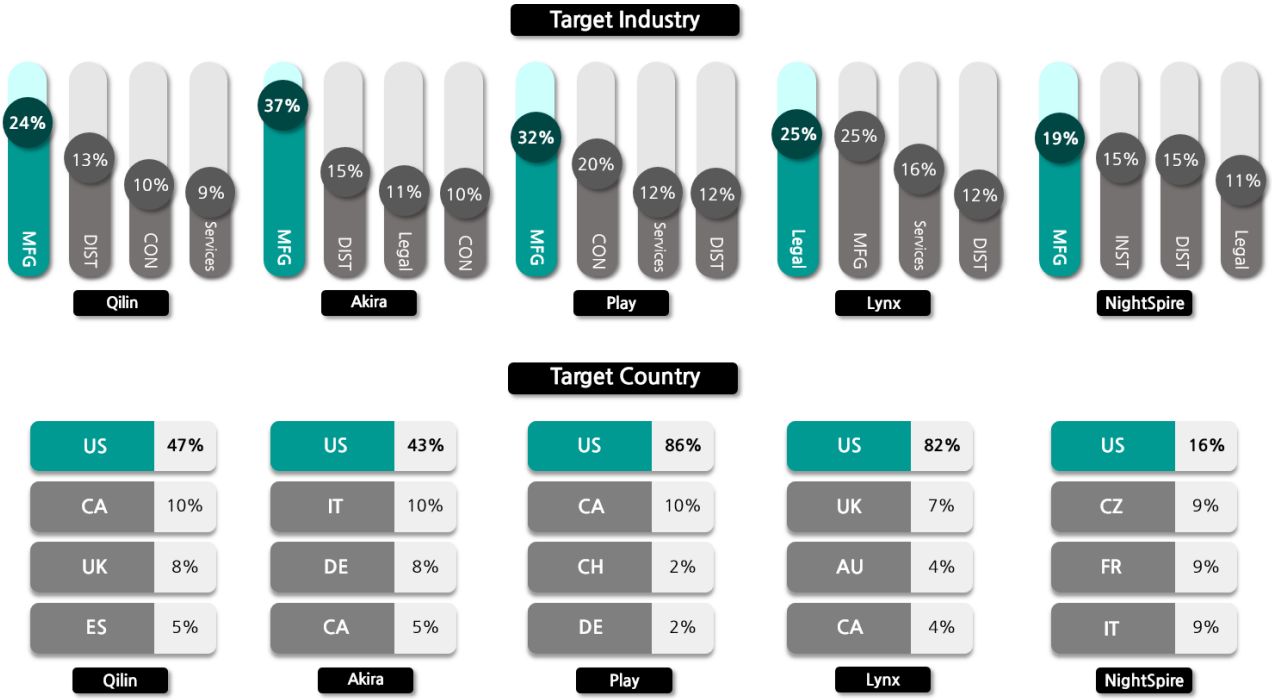


Figure 4. Current Status of Key Ransomware Attacks by Industry/Nation

In April, the Qilin group, which launched an attack on the American accounting firm Richmond CPA, leaked approximately 183GB of internal documents, including contracts, tax invoices, and payroll statements. In April alone, they posted a total of 74 victims. The surge in attacks is believed to be linked to the shutdown of the RansomHub service in early April, which led numerous affiliated attackers to join the Qilin faction. There are also allegations of connections with the North Korea-linked threat group Moonstone Sleet, particularly given the similarities in the distribution methods used by Moonstone Sleet's previously employed FakePenny ransomware, necessitating heightened vigilance.

In April, the Akira Group launched a cyberattack on TrussWorks International, a U.S.-based manufacturing and assembly service provider, resulting in the exfiltration of 13GB of sensitive data. This compromised data included not only personal information such as employee and customer contacts, telephone numbers, and addresses but also financial records and confidential non-disclosure agreements. In a separate incident, it has been reported that Santa Cruz Properties, a real estate services company, was similarly targeted, leading to the leakage of 15GB of data encompassing financial documents and contracts.

The Play group has been detected attempting to infiltrate systems by exploiting a Windows CLFS privilege escalation vulnerability (CVE-2025-29824). Following an attack on a public Cisco ASA [2]device vulnerability, there was confirmation of an attempt to implant their custom-developed information-stealing malware, Grixba, to gather internal network data and erase traces of their activity. Although no ransomware was deployed, the urgency to continuously monitor this situation arises from the possibility that not only the Play group but also other entities might have exploited this vulnerability before it was patched.

In April, the Lynx Group perpetrated an attack on Southern Ag LLC, an American agricultural consulting firm, compromising its internal operational systems and exfiltrating approximately 50GB of data, including financial documents, client data, and confidential records. Another victim of their cyber operations was Vicaraga Court Solicitors, a UK-based legal services provider, where emails and certain contracts were exposed on DLS Historically, this group has acquired the source code for INC ransomware, utilizing it in their operations. Recently, their attacks have evolved to incorporate the Lumma Infostealer, demonstrating a sophisticated amalgamation of information theft tools in their cyber arsenal.

NightSpire, a newly established group that commenced operations in March 2025, disclosed that it had targeted Nippon Ceramic, a Japanese ceramics manufacturer, in April, absconding with 45GB of technical design documents and production-related files. The purloined data was subsequently exposed on a dark web leak platform. Furthermore, towards the end of April, NightSpire infiltrated Melco Capital, a financial services firm based in Singapore, and exfiltrated approximately 1.8TB of financial information and internal documents. Recently, NightSpire has rapidly expanded the scope of its damages over the past few weeks.

[2] Cisco ASA: Cisco network security appliance providing firewall, intrusion detection/prevention, and VPN functionalities.

■ Focused Analysis on Ransomware

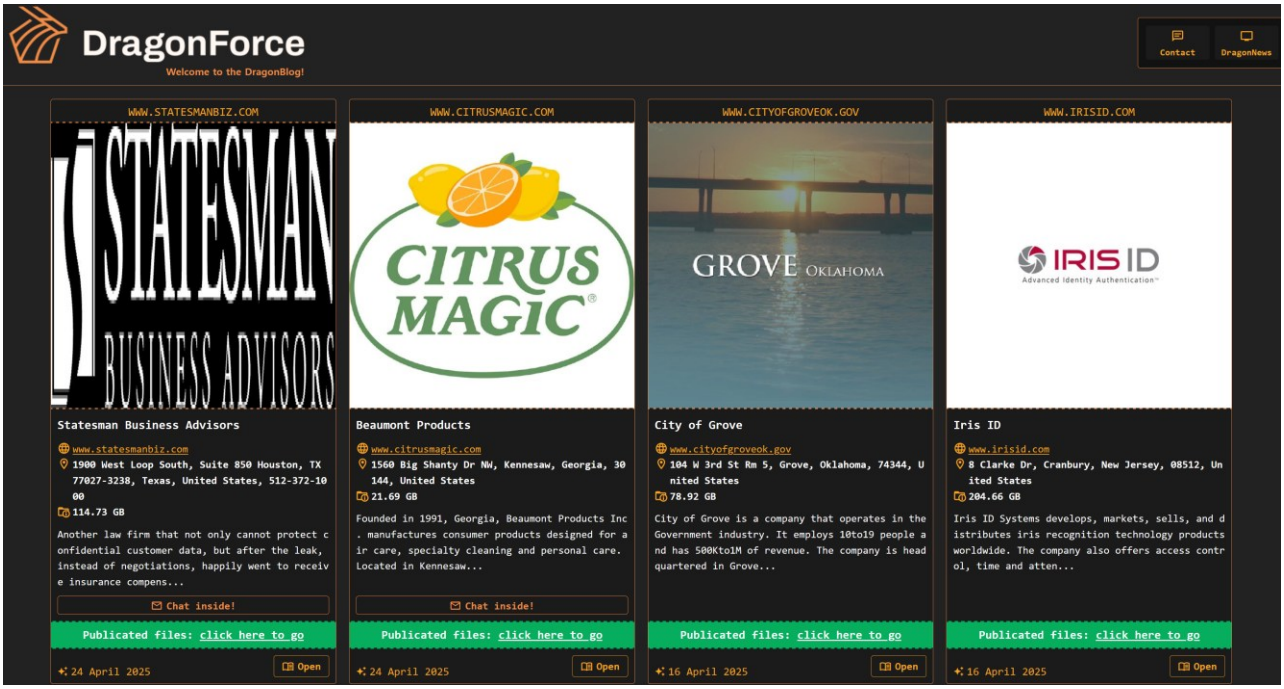


Figure 5. DragonForce Dark Web Leak Site

The DragonForce group commenced its operations in December 2023, consistently posting up to ten victims monthly. In June 2024, they uploaded a recruitment post on the Russian dark web hacking forum, RAMP, and have continued to update this post, introducing new services and detailing updates to their ransomware versions.

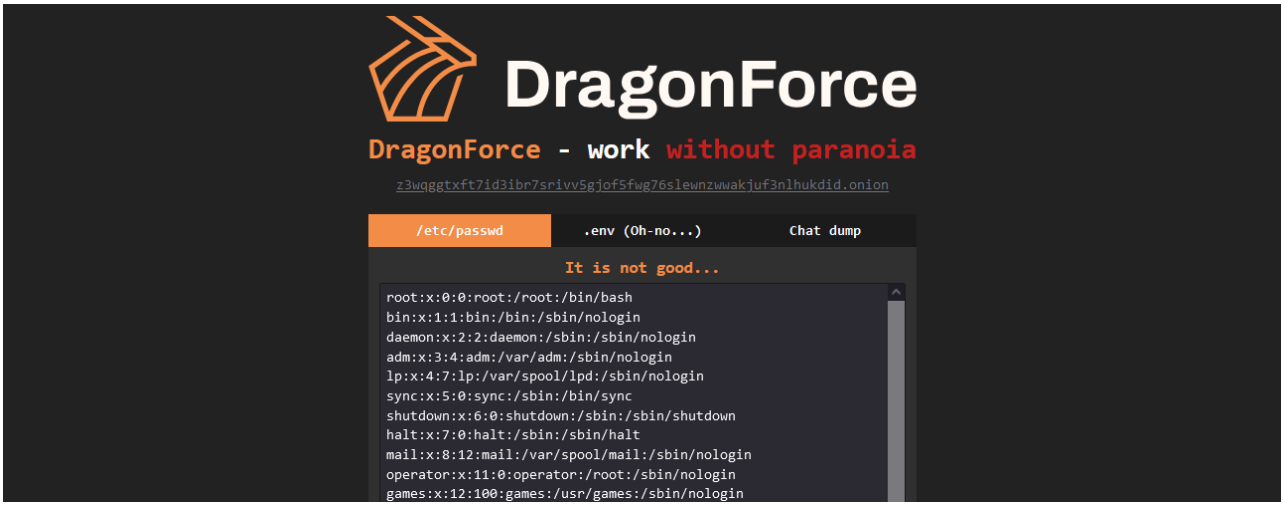


Figure 6. Hacked BlackLock Leak Site

In March 2025, DragonForce exploited the infrastructural security vulnerabilities of a rival group to hack the DLS of BlackLock and Mamona R.I.P. At that time, BlackLock's operational environment was known to be poorly secured, a fact that was widely recognized by various forum users, who speculated that DragonForce targeted this weakness for their hacking attempt. Following the hack, Mamona's leak site was completely deactivated, and BlackLock's site was altered to display promotional messages and logos for DragonForce.

Figure 7. RansomHub DLS Hosting Configuration

In April, there was evidence that DragonForce was attempting to promote itself through associations with other ransomware groups. At that time, RansomHub decided to delegate the operation of its infrastructure to DragonForce, and a related configuration page was made public. This was interpreted as an indication that both parties were indeed collaborating and reorganizing the infrastructure. This interpretation was influenced by the fact that RansomHub's dark web leak site was deactivated around the same period. However, the restored RansomHub leak page subsequently displayed only the phrase "RansomHub R.I.P. (03.03.2025)", and a user named 'hexcat' claimed that "RansomHub has been merged into DragonForce." This assertion raised the possibility that the relationship was not merely collaborative but constituted an acquisition by DragonForce.

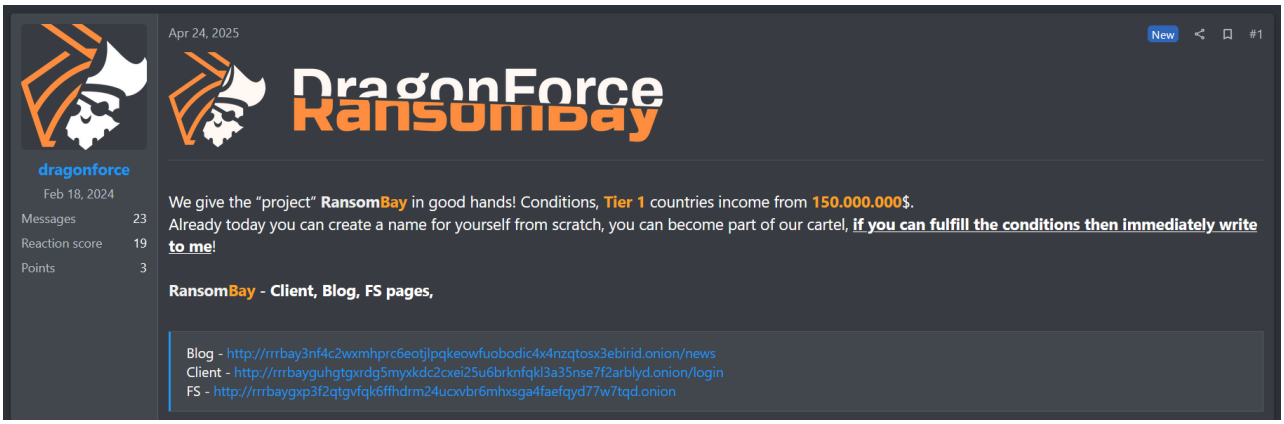


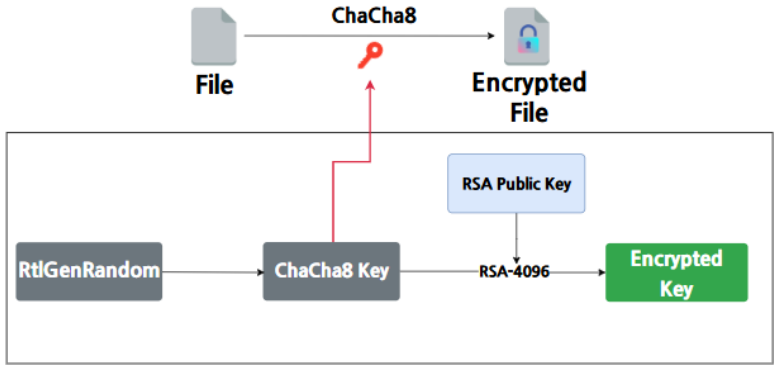
Figure 8. Promotional Material for RansomBay

The ransomware group known as DragonForce has begun to refer to itself as a "cartel" in an effort to expand its operational domain. It has declared that its affiliates may utilize the same infrastructure yet operate under distinct brands, with a new brand named RansomBay commencing activities from April. Recently, DragonForce has demonstrated strategic activities that transcend mere financial extortion, such as hacking the infrastructure of rival groups to exploit it as a promotional tool or to unveil new business structures. These maneuvers are rapidly broadening their foothold within the cyber threat ecosystem. This report aims to share an analysis of DragonForce ransomware, predicated on this background, to prepare for the impending threats.

DragonForce Ransomware

Encryption Key

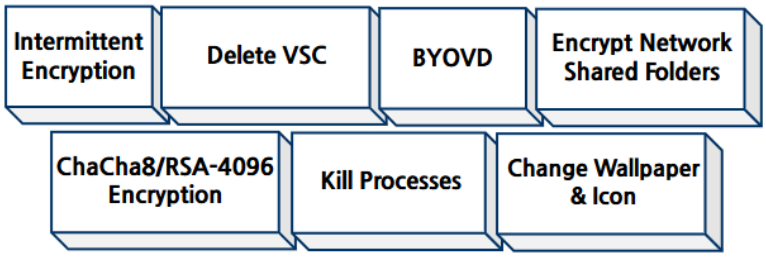
Encrypt files with ChaCha8 algorithm and protect the key with RSA-4096



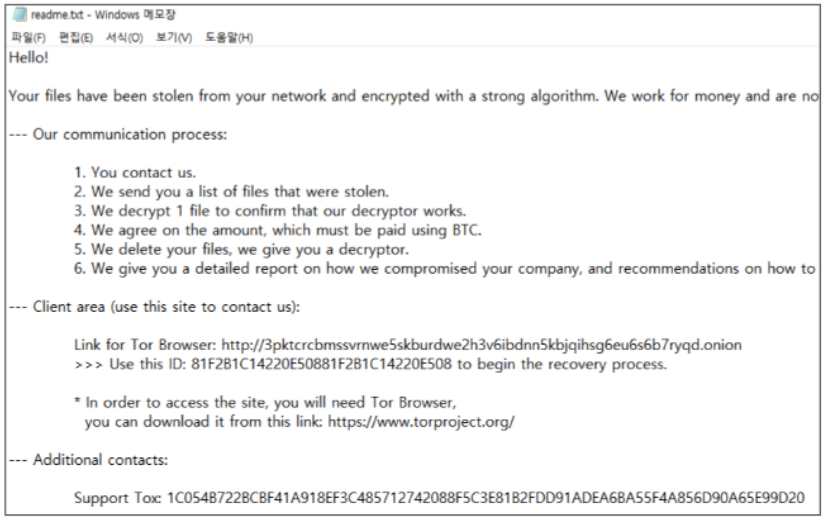
Encryption Method

2MB or less: Encrypt the entire file
more than 2MB and 10MB or less: Encrypt the first 3MB of the file
more than 10MB: Encrypt 50% of total size

Features



Ransom Note


readme.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

Hello!

Your files have been stolen from your network and encrypted with a strong algorithm. We work for money and are no

--- Our communication process:

1. You contact us.
2. We send you a list of files that were stolen.
3. We decrypt 1 file to confirm that our decryptor works.
4. We agree on the amount, which must be paid using BTC.
5. We delete your files, we give you a decryptor.
6. We give you a detailed report on how we compromised your company, and recommendations on how to

--- Client area (use this site to contact us):

Link for Tor Browser: http://3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd.onion
>>> Use this ID: 81F2B1C14220E50881F2B1C14220E508 to begin the recovery process.

* In order to access the site, you will need Tor Browser,
you can download it from this link: https://www.torproject.org/

--- Additional contacts:

Support Tox: 1C0548722BCBF41A918EF3C485712742088F5C3E81B2FDD91ADEA6BA55F4A856D90A65E99D20

readme.txt

Extension

.dragonforce_encrypted

Production Language

C/C++

Figure 9. Overview of DragonForce Ransomware

DragonForce Ransomware Strategy

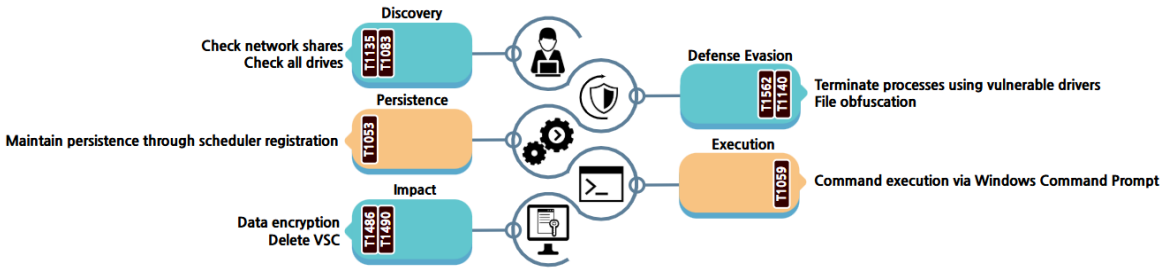


Figure 10. DragonForce Ransomware Attack Strategy

DragonForce ransomware employs a method wherein it encodes various strings used in logs or commands for backup copies, storing them encoded and decoding them as needed. Furthermore, it encrypts and stores essential data and configuration values required for execution, such as desktop backgrounds and icons, decrypting these upon the ransomware's activation. The functionality of the ransomware is determined based on the decrypted configuration values and the execution arguments input at the time of its launch.

The DragonForce ransomware is capable of configuring its encryption targets and methods through the utilization of various execution arguments, and it can permit the creation of log files or allow duplicate executions. However, according to the default settings encrypted within the ransomware itself, some arguments are merely verified and not utilized. The parameters and functions that are actually examined are as follows in the table below.

Parameters	Description
-p <path>	Encrypt Only Specified Paths
-m [all/local/nt/backups]	Configure Encryption Mode
-log <path>	Generate Log Files in Specified Paths
-size <percent>	Configure Partial Encryption Ratio
-nomutex	Allow Duplicate Executions

Table 1. Execution Parameters of DragonForce Ransomware

In instances where certain execution arguments are not applied, this is predominantly due to the configuration values stored within the ransomware itself. The ransomware possesses encrypted configuration settings utilizing the ChaCha8 algorithm, which are decrypted to determine the execution options of the ransomware. These stored configuration values are employed for tasks such as file encryption and process termination. Additionally, the initial section of the log file primarily stores these configuration settings of the ransomware, and the configuration values according to the stored log file are as follows in the table below.

Parameter	Description
build_key	Set Log File Encryption Key
custom_icon	Enable Encrypted File Icon Change
custom_wallpaper	Enable Desktop Wallpaper Change
custom_extension	Set Encryption Extension
time_sync	Enable System Time Synchronization
encrypt_mode	Set Default Encryption Mode (all, local, nt, backups)
full_encrypt_threshold	Set Full File Encryption Threshold
header_encrypt_threshold	Set File Header Encryption Threshold
header_encrypt_size	Set File Header Encryption Size
other_encrypt_chunk_percent	Set Partial Encryption Ratio
encrypt_file_names	Enable Base32 Encoding of Original Filenames
schedule_job	Enable Task Scheduler Registration
job_executable	Set Task Scheduler Executable Path
job_title	Set Scheduler Task Name
job_description	Set Scheduler Task Description
job_start	Set Scheduler Task Start Time
kill	Enable Process Termination
use_sys	Enable Use of BYOVD [3]Technique
priority	Set Target Processes for Termination
whitelist	Enable Encryption Exclusions
path	Set Encryption Exclusion Folders
ext	Set Encryption Exclusion Extensions
filename	Set Encryption Exclusion Filenames

Table 2. Configuration Settings of DragonForce Ransomware

[3] BYOVD: technique that leverages legitimately signed yet vulnerable drivers to bypass security solutions and execute malicious operations.

To facilitate seamless file encryption, processes stored in the configuration settings are terminated as a priority. The ransomware analyzed was found to contain a list of processes corresponding to those detailed in the table below.

process
MsMpEng.exe, sql.exe, oracle.exe, ocssd.exe, dbsnmp.exe, synctime.exe, agntsvc.exe,isqlplussvc.exe, xfssvccon.exe, mydesktopservice.exe, ocautoupds.exe, encsvc.exe, firefox.exe, tbirdconfig.exe, mydesktopqos.exe, ocomm.exe, dbeng50.exe, sqbcoreservice.exe, excel.exe, infopath.exe, msaccess.exe, mspub.exe, onenote.exe, outlook.exe, powerpnt.exe, steam.exe, thebat.exe, thunderbird.exe, visio.exe, winword.exe, wordpad.exe, notepad.exe, calc.exe, wuauclt.exe, onedrive.exe, SQLAGENT.exe, sqlservr.exe, SQLWriter.exe

Table 3. Processes Subject to Termination

While one could simply acquire process handles and terminate them, enabling the use_sys option causes this approach to exploit vulnerabilities in the truesight.sys and rentdrv2.sys drivers to terminate processes. By harnessing each driver's arbitrary termination capability, it evades detection by security solutions. The truesight.sys driver—a module of Adlice Software's RogueKiller Antirootkit providing rootkit detection and removal—was discovered to contain a flaw in versions up to 3.4.0 that permits arbitrary process termination. Similarly, rentdrv2.sys, used by the Chinese networking platform company Hangzhou Shunwang Technology, was found to possess an analogous vulnerability allowing arbitrary process termination. Although specific versions of rentdrv2.sys have not been disclosed, its developer claimed in December 2024 that the vulnerability had been remediated. Both drivers have since been included in the policy for blocking vulnerable drivers.

```
switch ( use_sys_flag )
{
  case 0:
    goto LABEL_26;
  case 1:                                   // truesight.sys | terminate process (0x22E044)
    v8 = DeviceIoControl(hDevice: hDevice, dwIoControlCode: 0x22E044u, lpInBuffer: &InBuffera, nInBufferSize: 4u, lpO
    break;
  case 2:                                   // rentdrv2.sys | terminate process (0x22E010)
    lpInBuffer[1] = InBuffera;
    lpInBuffer[0] = 1;
    v8 = DeviceIoControl(hDevice: hDevice, dwIoControlCode: 0x22E010u, lpInBuffer: lpInBuffer, nInBufferSize: 0x808u,
    break;
  default:
    goto LABEL_26;
```

Figure 11. Termination of Processes Utilizing BYOVD

Additionally, in order to prevent users from arbitrarily restoring encrypted files, backup copies are deleted. The command used to delete these backup copies is as follows.

```
cmd.exe /c C:\\Windows\\System32\\wbem\\WMIC.exe shadowcopy where "ID='%s'" delete
```

Table 4. Commands to Delete Backup Copies

Following the deletion of backup copies, the encryption target is determined based on the encryption mode set by the -m execution argument. The modes are differentiated into local, which encrypts connected drives; nt, which encrypts the "ADMIN$" folder among network shared resources; and all, which encrypts both drives and network shared resources. Additionally, there exists a mode named backups, which, if selected, results in the termination of the process without encrypting any files. Utilizing the -p execution argument enables the encryption of specific folders, and in the absence of either the -m or -p arguments, the default settings specified in the configuration are employed.

Once the encryption targets have been established, each directory is traversed to ascertain whether it corresponds to an exception item. These exception items are stored in the configuration settings, and based on these criteria, it is determined whether a directory qualifies as an exception. Upon completion of the directory verification, the presence of files within each directory is then scrutinized to determine if they constitute exception items. The encryption exceptions under consideration are as delineated in the table below.

Directory Name	File Extension and File Name
tmp, winnt, temp, thumb, $Recycle.Bin, $RECYCLE.BIN, System Volume Information, Boot, Windows, perflogs, Public	.exe, .dll, .lnk, .sys, .msi, .bat, .dragonforce_encrypted, readme.txt

Table 5. Exceptions to Encryption

The methodology for file encryption is determined based on the file's extension and size. Files associated with databases undergo complete encryption regardless of their size, whereas files related to virtual machines are encrypted only for the initial 20% of their content, irrespective of the file size. The corresponding file extensions for each category are delineated in the table below.

Extension
.dadigrams, .sqlite, .db, .sas7bdat, .daschema, .sqlite3, .abcddb, .sqlite, .nrmlib, .db-wal, .db-shm, .dacpac, .accdw, .xmlff, .kexis, .kexic, .fmp, .sl, .accft, .accdt, .accdr, .accde, .accdc, .accdb, .fmp12, .temx, .rodx, .rctd, .nwd, .kexi, .itd, .grd, .epim, .dtsx, .dlis, .wmd, .mdn, .maw, .lut, .kdb, .icr, .icg, .hjt, .fm5, .db2, .adn, .abx, .abs, .xld, .xdb, .wrk, .wdb, .vvv, .vpd, .vis, .v12, .usr, .udl, .udb, .trm, .trc, .tps, .tmd, .sql, .spq, .sis, .sdf, .sdb, .scx, .sbf, .rsd, .rpd, .rod, .rbf, .qvd, .qry, .pnz, .pdm, .pdb, .pan, .p97w, .p96, .owc, .orx, .oqy, .odb, .wyn, .yf, .wnv2, .nsf, .ns4, .ns3, .ns2, .nnt, .ndf, .myd, .mwb, .mud, .mrg, .mpd, .mdf, .mdb, .mav, .mas, .mar, .maq, .maf, .lwx, .lgc, .kdb, .jtx, .jet, .itw, .ihx, .idb, .his, .hdb, .gwi, .gdb, .frm, .fpt, .fp7, .fp5, .fp4, .fp3, .fol, .fmp, .fic, .fdb, .fcd, .exb, .ecx, .eco, .dxl, .dsk, .dqy, .dp1, .ddl, .dcx, .dct, .dcb, .dbx, .dbv, .dbt, .dbs, .dbc, .db3, .dad, .cpd, .cma, .ckp, .cdb, .cat, .bdf, .btr, .ask, .alf, .ora, .arc, .adp, .adf, .ade, .adb, .4dl, .4dd, .mdt, .nv, .ib, .db, .te

Table 6. Extensions Related to Databases

Extension
.vdi, .vhd, .vmdk, .pvm, .vmsn, .vmsd, .nvram, .vmx, .raw, .qcow2, .subvol, .bin, .vsv, .avhd, .vmrs, .vhdx, .avdx, .vmcx, .iso

Table 7. Extensions Related to Virtual Machines

Remaining files are encrypted fully or partially depending on the full_encrypt_threshold (2 MB) and header_encrypt_threshold (10 MB). Files ≤ 2 MB are fully encrypted; files > 2 MB and ≤ 10 MB have only their first 3 MB encrypted; and files > 10 MB are encrypted up to 50 % of their total size.

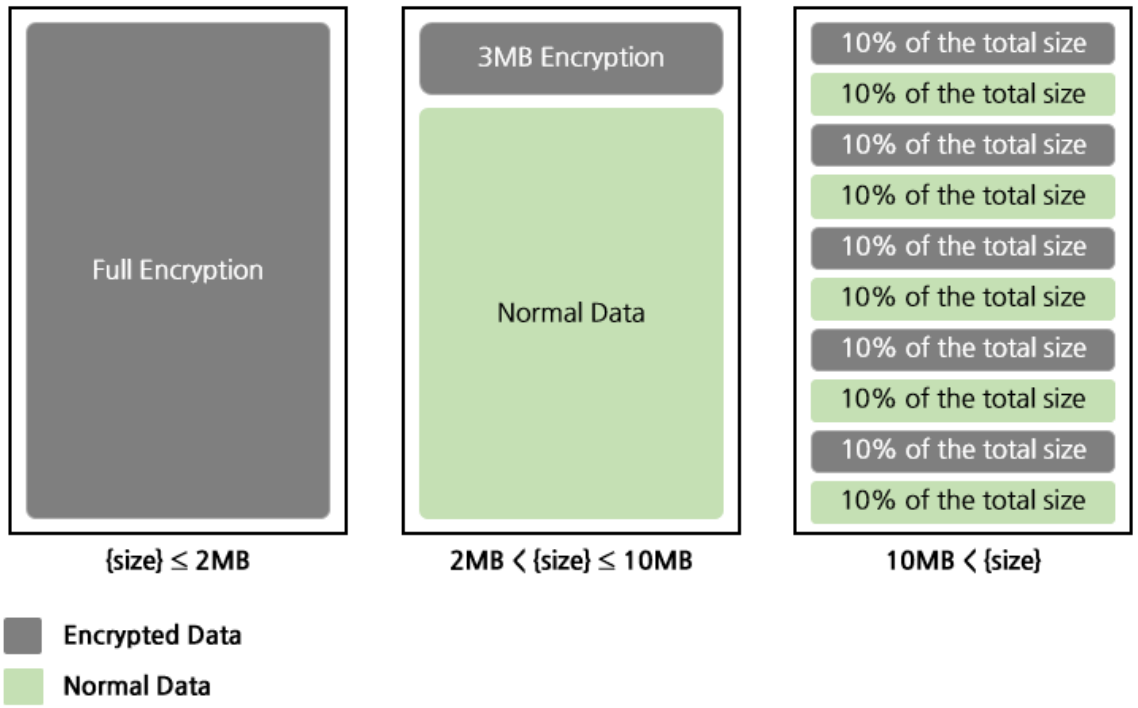


Figure 12. File Encryption Methods by Size

The encryption algorithm employed is ChaCha8, and the utilized key and Initialization Vector (IV) are safeguarded using an RSA-4096 public key, subsequently appended to the end of the encrypted file. Following the encryption of the file, an encryption extension is added. Should the option 'encrypt_filenames' be activated, not only is the encryption extension appended, but the filename itself is encoded. Although Base32 is the encoding method used, it diverges from the standard character set, instead employing the bespoke character set "gwfn6l3bk45o2zecvi7xtyqrpsudmahj" to encode the original filename before appending the encryption extension.

Figure 13. Altered Desktop Background

Following the encryption of files, ransomware alters the desktop background and the icons of encrypted files to those of stored images and icon files. The wallpaper is saved at the path "C:\Users\Public\wallpaper_white.png," and the icon image is stored at "C:\Users\Public\icon.ico."

In addition to its primary functions, it has been confirmed that the ransomware possesses the capability to register itself within the task scheduler for execution. Should such a configuration exist, the current ransomware copies itself to the path stored in the job_executable setting. Subsequently, it creates a task using the value stored in job_title as the task name and the content of job_description as the task description, scheduling the task to initiate at the time specified in job_start.

DragonForce Ransomware Mitigation Strategies

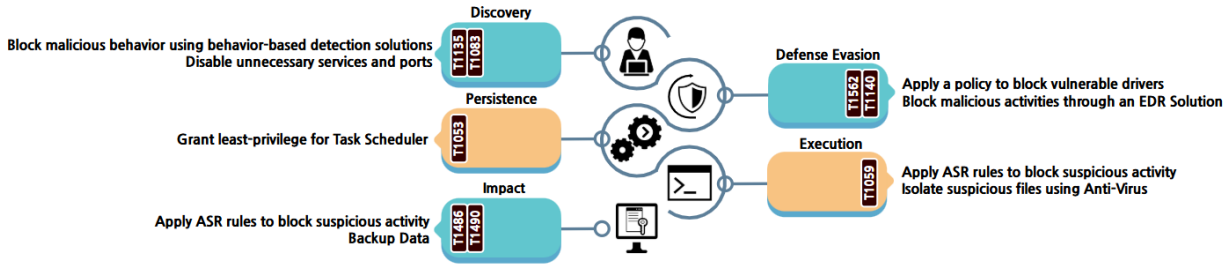


Figure 14. Response Strategies for DragonForce Ransomware

The DragonForce ransomware utilizes the Windows command prompt to execute the deletion of backup copies. Consequently, by activating ASR[4] rules, one can thwart malicious activities by blocking anomalous processes. Furthermore, as the ransomware replicates itself to specific locations for task registration or stores programs in temporary folders, it is feasible to isolate suspicious files using Anti-Virus software.

In order to encrypt network shared folders, the current system's internal network bandwidth is scrutinized, and attempts are made to access connectable shared folders. Furthermore, in the case of file encryption, all drives are examined and, based on the execution arguments, the drives to be encrypted are distinguished. Consequently, through the deployment of behavior-based detection solutions, it is feasible to thwart the malicious activities of attackers.

Despite possessing legitimate signatures, the exploitation of vulnerable versions of the drivers truesight.sys and rentdrv2.sys to circumvent security devices and attempt process termination necessitates the implementation of a policy to block these vulnerable drivers. This issue can be addressed through the adoption of a vulnerable driver blocking policy, and Microsoft has already included these two susceptible drivers in its list of blocked drivers. By applying this guideline to the system, one can prevent the exploitation of these vulnerable drivers. Moreover, the files and commands required for malicious activities exist in encrypted or encoded forms, and are decrypted and decoded just before use. Therefore, it is imperative to block these malicious activities through an EDR[5] solution.

In order to prevent users from arbitrarily restoring encrypted files, the system deletes all existing backup copies before encrypting the files. Activation of ASR rules can block the processes of deleting backup copies and encrypting files. Furthermore, it is imperative to disperse backup copies across separate networks or storage facilities, ensuring that recovery is feasible even if the system becomes encrypted.

[4] ASR (Attack Surface Reduction): protection feature that blocks specific processes used by attackers and prevents execution of unauthorized processes.

[5] EDR (Endpoint Detection and Response): solution that detects, analyzes, and responds in real time to malicious activities on endpoints—including computers, mobile devices, and servers—to prevent the spread of damage.

IoCs

Hash(SHA-256)
d06b5a200292fedcfb4d4aecac32387a2e5b5bb09aaab5199c56bab3031257d6
70afd8efb34382badead93ae104d958256de6be8054227ccc85fe95d5c5f9db0

■ Reference Sites

• Guide Point Security (https://www.guidepointsecurity.com/blog/ransomsnub-ransomhubs-affiliate-confusion/)

• The Hacker News (https://thehackernews.com/2025/05/play-ransomware-exploited-windows-cve.html)

• The Hacker News (https://thehackernews.com/2025/05/qilin-leads-april-2025-ransomware-spike.html)

• BleepingComputer (https://www.bleepingcomputer.com/news/security/everest-ransomwares-dark-web-leak-site-defaced-now-offline/)

• Symantec (https://www.security.com/threat-intelligence/play-ransomware-zero-day)

• GitHub (https://github.com/keowu/BadRentdrv2)

• UNIT 42 (https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/)

• Microsoft (https://learn.microsoft.com/ko-kr/windows/security/application-security/application-control/app-control-for-business/design/microsoft-recommended-driver-block-rules)

Special Report

Zero Trust Security Strategy: Identifiers and Identity Management

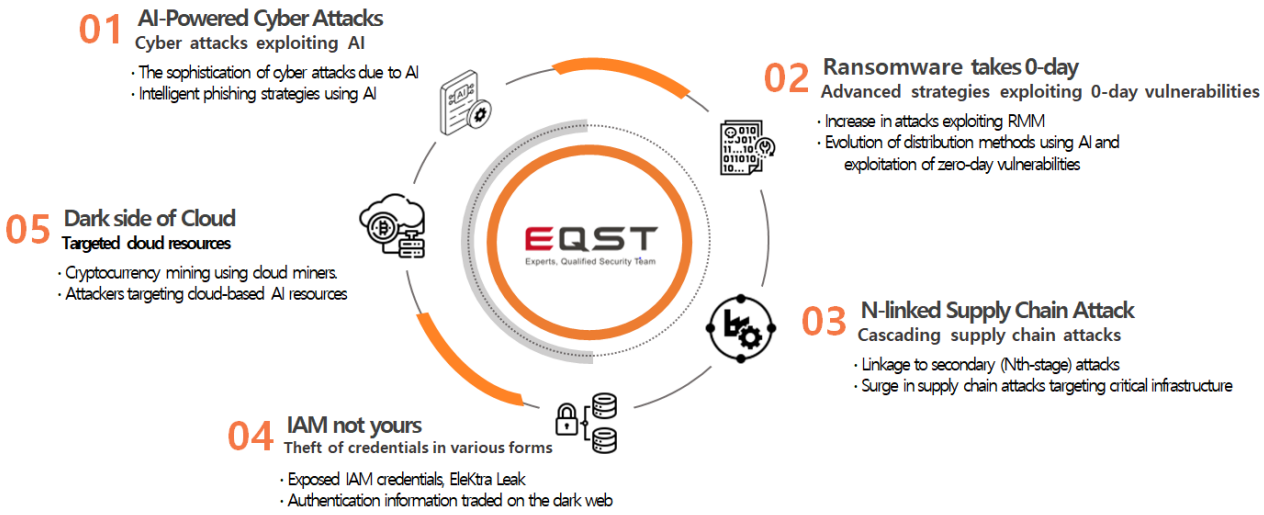
Byung-gwon Hwang / Security SI Business team, Senior Manager

■ 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.



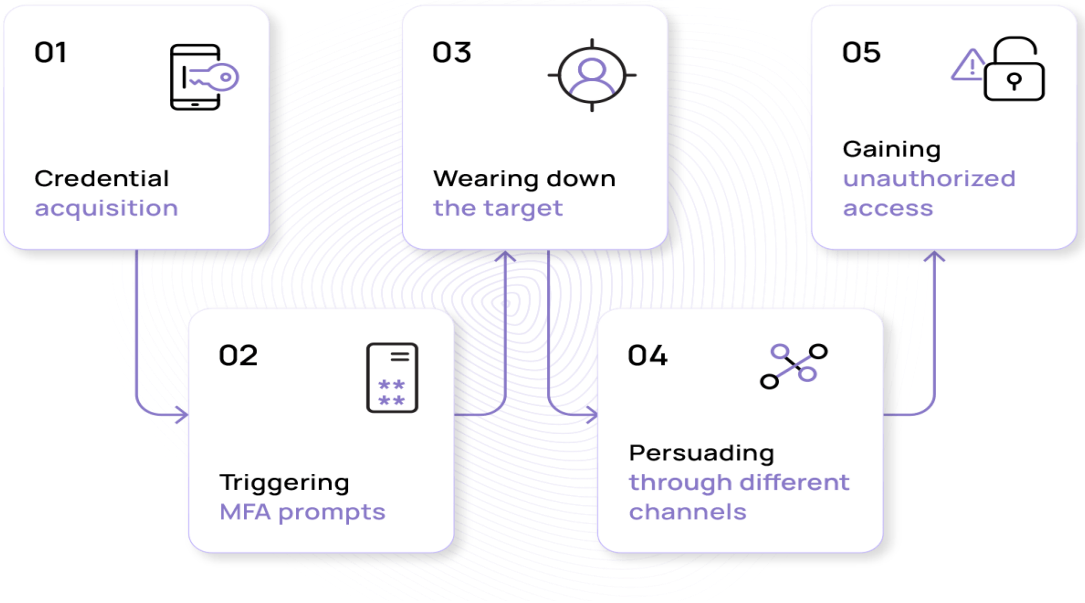
Source: SK Shieldus EQST, "2025 Security Threat Forecast Report"

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.

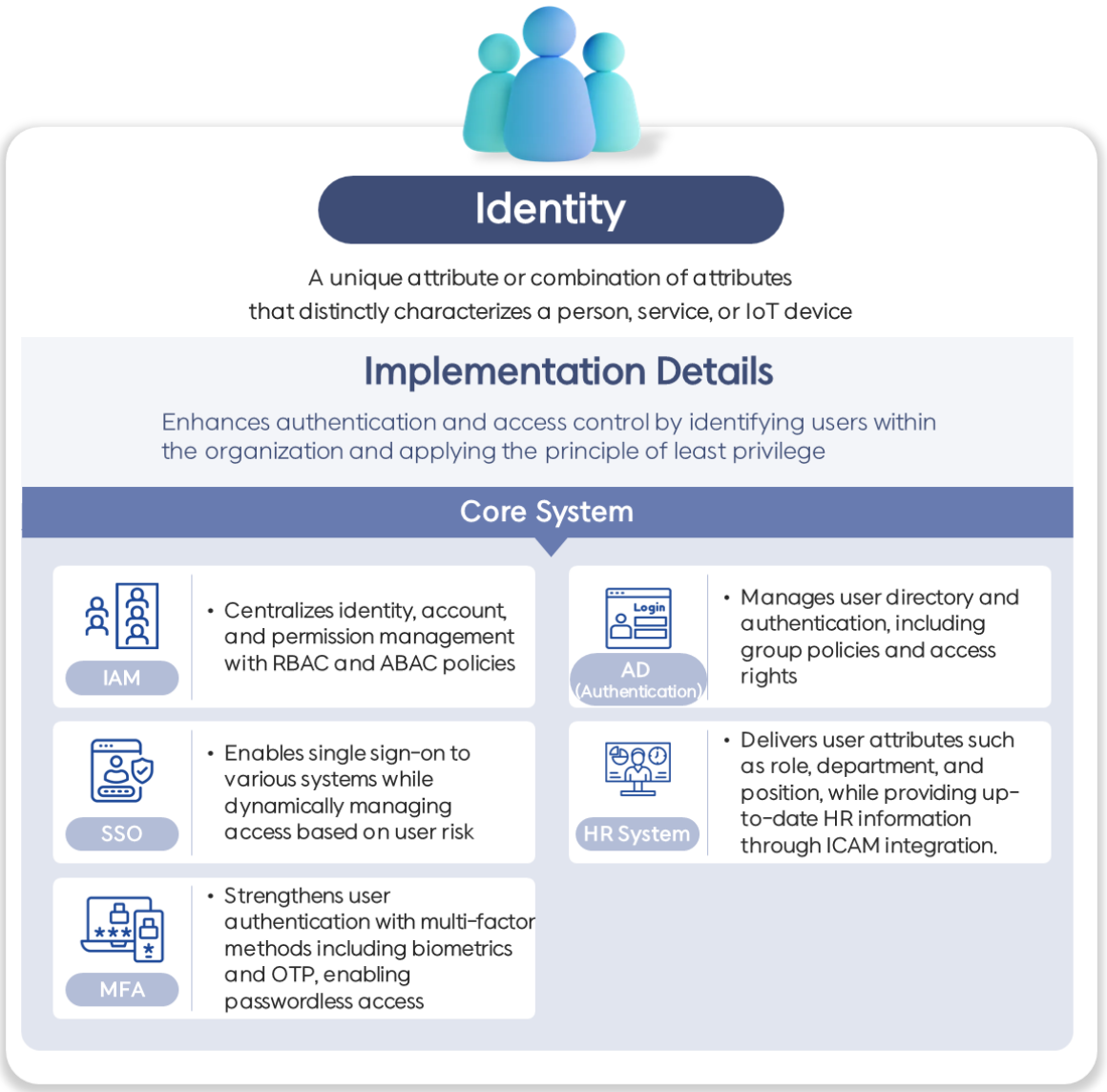
Risk assessment is utilized as critical data for the enhancement of authentication and the authorization process, and it must facilitate immediate responses through real-time monitoring.

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.

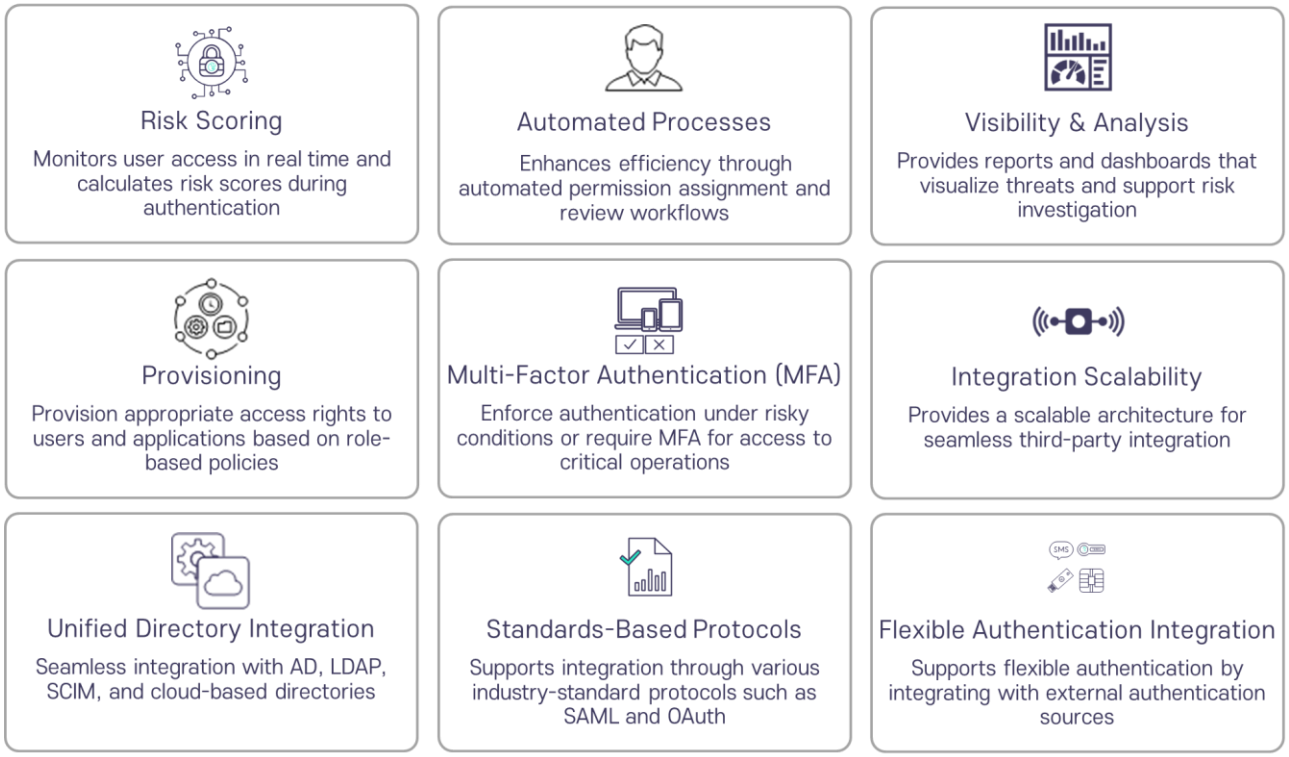


Figure 4. Key Features of Zero Trust-Based SSO/IAM

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"

EQST INSIGHT

2025.05

SK shieldus

SK Shieldus Inc. 4&5F, 23, Pangyo-ro 227beon-gil, Bundang-gu, Seongnam-si, Gyeongggi-do, 13486, Republic of Korea
https://www.skshieldus.com

Publisher: SK Shieldus EQST business group
Production: SK Shieldus Marketing Group