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
07

SK shieldus

Contents

Headline

Strategies for Achieving Security Visibility and Addressing Gray Zone Vulnerabilities

Sung-kwang Baek, SK Shieldus

■ Overview

We have transcended an era of change and entered an 'era of transformation.' The advent of the internet in the 1990s catalyzed an explosive increase in information dissemination and communication during the process of system development and service provision. Based on these services, we now exchange a plethora of information, sustaining the lives of modern individuals.

Companies that provide services have traditionally managed their IT resources within on-premise environments, such as proprietary data centers and servers. However, with the burgeoning growth of the cloud market and advancements in technology, these companies are now able to utilize IT resources with greater flexibility according to their needs, thereby integrating cloud solutions into their operations and services. Recently, the rapid evolution of artificial intelligence (AI) technologies has led to their integration across a multitude of sectors. Corporations are adopting AI to enhance efficiency and reduce costs, while government and public institutions are easing and improving previously stringent network separation regulations to bolster AI capabilities and strengthen competitiveness. This is exemplified by initiatives such as the National Network Security Framework (N2SF) and the roadmap for improving network separation in the financial sector.

■ Hackers' Target: The Security Gray Zone

As the transition from on-premise environments to cloud and AI technologies accelerates, security vulnerabilities that organizations were previously unaware of are emerging. Hackers are exploiting these gaps for a variety of reasons, including financial gain, military objectives, and political motives.

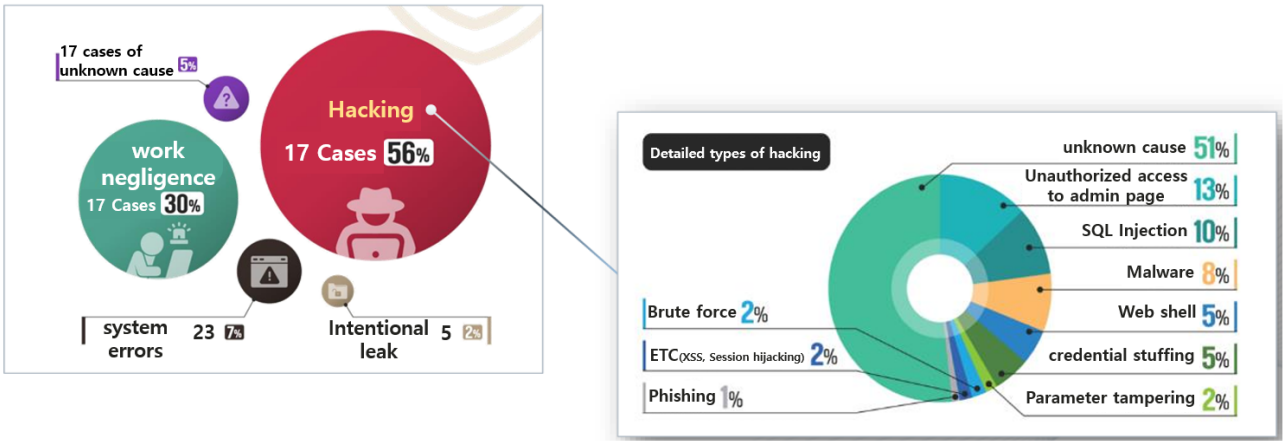
The concept of the "Gray Zone" in security arises from unmanaged and neglected assets, the absence of risk management activities, and human errors. Analyzing instances of security incidents reveals that the primary causes often include insufficient identification and remediation of vulnerabilities on service surfaces such as VPNs, as well as vulnerabilities in web and application platforms. Additionally, inadequate control over external internet access frequently results in work-related user PCs becoming infected with malware.

Enterprises are increasingly operating certain IT services through cloud platforms, and consequently, numerous security personnel are expressing difficulties in managing security within the cloud domain. This challenge arises from the fact that development departments can utilize cloud services with merely internal approval, often leaving the security departments unaware, resulting in a lack of security assessments. Furthermore, there is an absence of clear standards regarding which functions of which services should be scrutinized within the cloud environment and how the generated logs should be managed. This creates a "Gray Zone" of security invisibility, akin to peering into a cloud, which is frequently targeted by hacking incidents.

Cybersecurity incidents with financial motives continue to afflict various enterprises, including ransomware attacks on global healthcare entities such as UnitedHealth Group and Change Healthcare, the compromise of MFA accounts on the Snowflake cloud platform, and ransomware infections targeting Yes24. In the realm of international conflicts, both Ukraine and Russia have engaged in cyber warfare surrounding the Ukraine-Russia war (2022-present), executing DDoS (Distributed Denial of Service) attacks on governmental and financial institutions, deploying data-wiping malware like WhisperGate, hacking satellite communications, and conducting phishing operations to exfiltrate military data. Similarly, in the conflict between Israel and Hamas/Iran, there have been DDoS attacks targeting government and media services, alongside hacking attempts on power grid operators.

Since the armistice in 1953, our nation has been in a continuous state of confrontation with North Korea, a situation that has extended into the realm of cyberspace, where North Korean cyber assaults have been relentless. Notable incidents include the 7.7 Distributed Denial of Service (DDoS) attack in 2009, the 3.20 cyber terrorism event involving the hacking of financial institutions and broadcasters in 2013, the attempted hacking of Seoul's transportation and communication networks in 2019, and the attack on Korea Hydro & Nuclear Power in 2020. The recent BPF hacking incident involving telecommunications company S is also widely interpreted as part of the ongoing cyber security threats. Furthermore, with the escalating tensions between China and Taiwan, it is anticipated that there will be an increase in cyber attack attempts targeting our nation, given its strategic importance to the United States.

The methodologies employed by hackers are diverse; however, the targets of these attacks predominantly originate from vulnerabilities present within organizational systems. According to the "Directions for Strengthening Personal Information Security Management Systems" report released by the Personal Information Protection Commission in May 2025, it was revealed that 56% of domestic security incidents last year were attributed to hacking that exploited system vulnerabilities.



* Source: Personal Information Protection Commission (May 21, 2025)

Figure 1. Causal Categories of Personal Information Breach Incidents Last Year

When encountering news articles related to cybersecurity incidents, the unfamiliar terminology and technical explanations can often render comprehension challenging. However, the essence of most reports is that hacking occurs through system vulnerabilities, leading to information breaches. Hackers target the weakest link within an organization, namely the vulnerabilities in the system, to infiltrate.

■ Identifying and Bridging Security Gaps in the Gray Zone

Individuals pursue happiness through a healthy lifestyle, endeavoring to adhere to regular meals, sleep, and exercise. Furthermore, they maintain their health by undergoing regular medical check-ups, which facilitate the early detection and treatment of diseases that may otherwise go unnoticed.

To ensure robust cybersecurity within an organization, fundamental activities are indispensable. The cornerstone of security involves the operation of security solutions, the monitoring and response to security breaches, the establishment of an Information Security Management System (ISMS), and the management of risks. Furthermore, to address the security gaps, often referred to as the "Gray Zone," which emerge due to evolving technological environments, it is imperative to implement security strategies that incorporate new technologies.

1. Implementation and Operation of Security Solutions

Since the early 2000s, numerous experts have drawn an analogy between cybersecurity and a "castle" to elucidate its principles. This analogy involves distinctly demarcating the internal network of an organization from the external internet, akin to the separation of a castle's interior from the outside world. To thwart external threats, defensive mechanisms such as firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) are strategically deployed at the network perimeter. This approach mirrors the medieval fortress strategy, where high walls and moats were employed to prevent invasions.

When an organization embarks on the establishment of its cybersecurity framework, the foremost consideration must be the implementation of robust security solutions. Analogous to erecting fortifications and stationing guards at the gates to regulate ingress and egress, it is imperative to configure firewalls that delineate the internal network from external threats. Furthermore, to detect and intercept threats infiltrating from the outside, it is essential to deploy intrusion prevention systems such as Web Application Firewalls (WAF) and Intrusion Prevention Systems (IPS). Subsequently, the foundation for comprehensive security operations is laid by instituting measures for internal endpoint (PC) control, system access management, account administration, database encryption, and the establishment of backup and recovery systems.

A hacking incident typically unfolds through a sequence of steps that commence with breaching vulnerabilities, followed by information gathering on the compromised terminal (PC, server). Subsequently, the attacker searches for other vulnerable systems in the vicinity, installs malware or backdoors, deploys ransomware, exfiltrates data, and may even demand a ransom. The recent incidents have been characterized by the deployment of sophisticated and previously unknown malware, which poses significant challenges for detection by conventional antivirus solutions. Therefore, the implementation of Endpoint Detection & Response (EDR) systems, which are capable of detecting and responding to such malicious activities, is instrumental in addressing the uncharted "Gray Zone" that traditional security solutions have failed to illuminate, thereby enhancing visibility and security posture.

Due to the lack of experience among personnel or insufficient organizational funding, numerous gray areas have emerged even within cloud environments. Although security measures such as firewalls, Intrusion Prevention Systems (IPS), access controls, and log monitoring via CloudTrail are being implemented to safeguard cloud infrastructure, it remains challenging for organizations to clearly comprehend their operational security posture. To ensure security visibility within cloud services, it is imperative to employ Cloud Security Posture Management (CSPM) for real-time assessment of security status, as well as Cloud Workload Protection Platform (CWPP) solutions to detect, defend against, and manage vulnerabilities within workload execution environments. Furthermore, security events generated by various security solutions must be collectively aggregated through Security Information and Event Management (SIEM) systems, facilitating the correlation and analysis of events to identify and thwart intrusion attempts. Areas not covered by security solutions—such as the adequacy review of server access accounts and the evaluation of account permissions on service management pages—must be continuously managed using human resources in accordance with established standards and procedures.

2. Establishment of Security Management Framework and Risk Management Activities

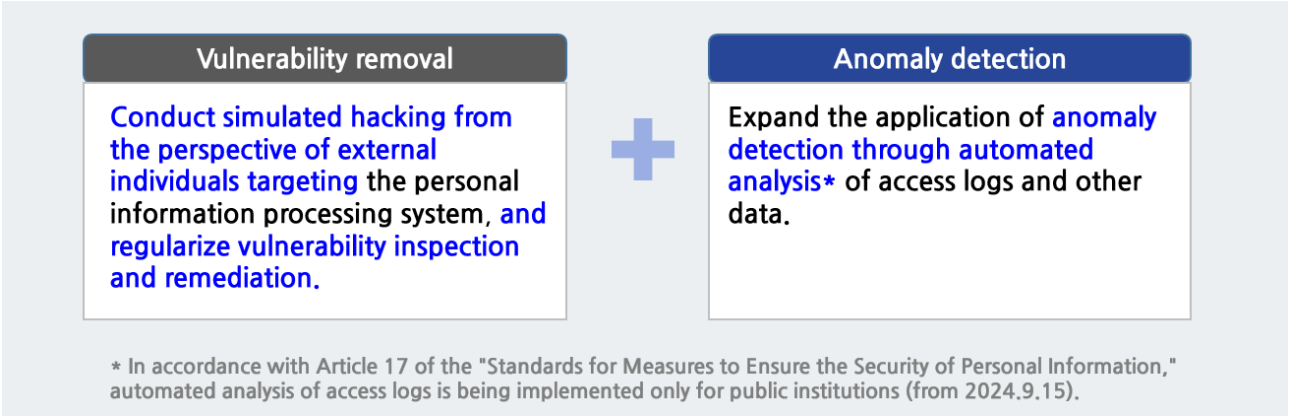
If constructing a fortress to shield the organization from external threats through security solutions is akin to building a castle, it is now imperative to establish a systematic management framework to operate it effectively. This involves formulating standards and regulations, assembling a dedicated team, and assigning roles such as chief security officer, watchtower guards, and sentinels to ensure smooth operation. Concurrently, it is essential to regularly inspect and maintain the robustness of defensive structures such as ramparts, waterways, and moats.

Cybersecurity is no exception. To safeguard internal systems and information assets, it is imperative to establish regulations, guidelines, and procedures, and to assemble an organization responsible for executing information security planning, solution operations, incident response, and security audits. An annual plan must be devised, and under the approval of the executive management, the planned security management should be implemented periodically (annually, quarterly, monthly, or daily).

Risk management activities encompass the identification of assets that require protection—such as systems, information, and personnel—and the assessment, elimination, and management of known vulnerabilities. The identification of assets must comprehensively include information, hardware, software, facilities, and personnel without omission.

In the identified systems, it is imperative to assess and eliminate known vulnerabilities, such as those cataloged under Common Configuration Enumeration (CCE) and Common Vulnerabilities and Exposures (CVE), as well as vulnerabilities present in source code, web, and mobile applications. In instances where functional elimination proves challenging, it is essential to devise plans for system replacement or functional enhancement. Concurrently, supplementary measures such as access control and post-incident monitoring must be implemented to fortify security.

When the introduction or modification of a new system occurs, updating the asset management register and eliminating vulnerabilities within the system constitute the most fundamental yet crucial procedures. The Personal Information Protection Commission, in its "Direction for Strengthening Personal Information Security Management Systems," identifies the elimination of vulnerabilities as the top priority in security measures.



* Source: Personal Information Protection Commission

Figure 2. Strategic Initiatives: ① Immediate and Technical Action Items (1)

Recently, even companies that have obtained ISMS certification have experienced security incidents, leading to frequent inquiries such as, "Why do incidents occur despite having certification?" The ISMS-P (Information Security Management & Personal Information System) serves as a 'framework' for structuring an organization's security activities. The certification process is akin to a health check-up, designed to assess the current status and address any deficiencies.

Just as one maintains a regimen of healthy eating, adequate sleep, and diligent exercise to preserve health, yet still encounters illness and health deterioration due to various environmental factors, so too must one enhance security annually by addressing deficiencies and vulnerabilities identified through the maintenance of ISMS-P certification from a preventive standpoint. This continuous improvement is essential to fortify cybersecurity defenses.

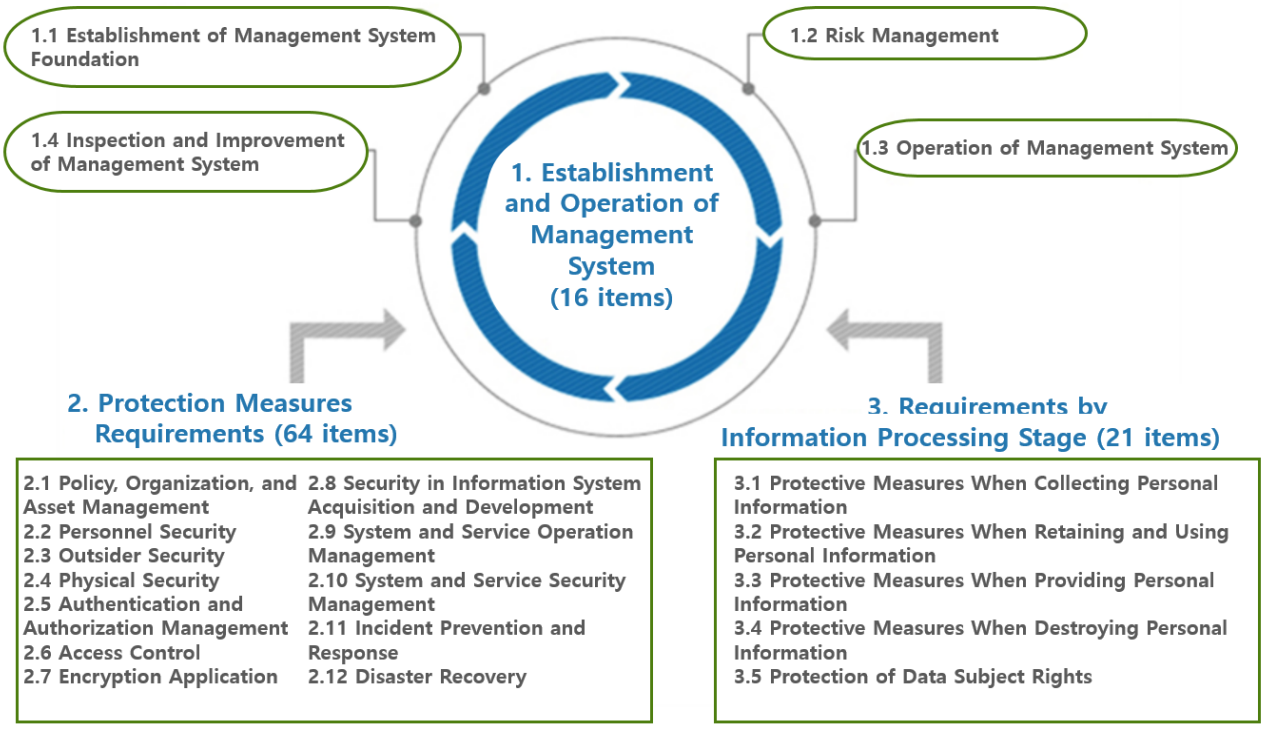


Figure 3. Korea Internet & Security Agency (KISA) Website > Introduction to ISMS-P Certification System > Certification Criteria

3. Identifying and Mitigating Security Vulnerabilities in the Gray Zone

The most powerful king in the history of Israel, David, succeeded in capturing the seemingly impregnable fortress of Jerusalem. Although it was a mountain stronghold surrounded by deep valleys, he infiltrated the interior of the fortress through a water supply tunnel that connected the outside to the inside. The fall of this formidable fortress was attributed to structural and managerial vulnerabilities.

The realm of organizational cybersecurity is no exception. Even with the implementation of robust security solutions and the establishment of an Information Security Management System for Personal Information (ISMS-P), coupled with annual audits, there may still exist unrecognized gray zones that become prime targets for hackers. Much like the strategic wisdom encapsulated in Sun Tzu's "Know the enemy and know yourself, and you will not be imperiled in a hundred battles," a clear understanding of the systems, assets, and data we must protect enables us to eliminate vulnerabilities and minimize exposure to attacks. Furthermore, by analyzing recent security incident types and attack patterns, and by evaluating systems from a hacker's perspective, these gray zones can be effectively mitigated.

The ISMS-P evaluates each item solely as 'adequate' or 'inadequate,' making it challenging to conduct a qualitative assessment of whether the security measures are 'sufficiently safe.' Consequently, it is an effective strategy to concurrently implement standards such as the Security Maturity Model or the MITRE ATT&CK Framework*, which provide a more nuanced evaluation.

label	CMMI	CMMC	C2M2
Purpose	Improve process maturity and efficiency	Assess cybersecurity maturity and DoD compliance	Enhance IT/OT cybersecurity and risk management
Application Area	All industries incl. software and services	Defense, DoD contractors (FCI/CUI)	Critical infrastructure and general industry
Structure / Scope	Up to 22 process areas	17 domains / 3–5 levels	10 domains / 350+ practices
Maturity Level	5 levels (Initial–Optimizing)	3–5 levels (Foundational–Expert)	4 levels per domain (MIL0–MIL3)
Evaluation Method	External review / Internal benchmarking	3rd-party audit / Self-assessment / DoD rule	Self + external / Domain-level scoring
Key Features	Integrated, optimized processes	NIST-aligned / Legally required	Practical, risk-based, balanced approach
Requirement	Optional (benchmarking standard)	Mandatory (for DoD partners)	Optional (recommended for CI sectors)

Table 1. Comparison of Maturity Models - Summary of Perplexity Data

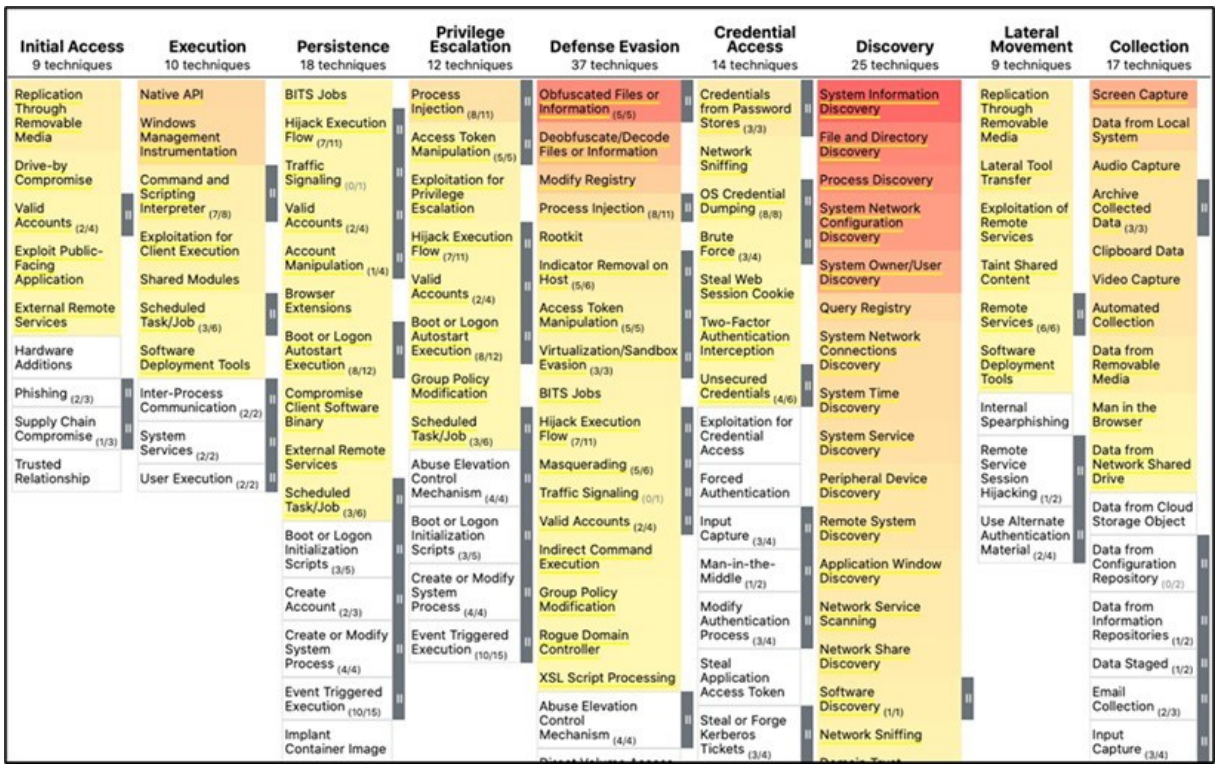


Figure 4. Excerpt from MITRE ATT&CK Matrix - Navigator

* MITRE ATT&CK Framework: The MITRE ATT&CK, an acronym for Adversarial Tactics, Techniques, and Common Knowledge, is a systematically organized knowledge base matrix that categorizes the tactics, techniques, and procedures (TTPs) employed by adversaries in real-world scenarios.

Finally, it is imperative that an organization's cybersecurity framework is underpinned by clearly defined 'objectives and strategies.' In the absence of such objectives, it becomes challenging to maintain consistency and efficacy in security measures. Objectives serve as the benchmark for risk mitigation and the prioritization of resources, thereby facilitating more efficient and effective security operations.

A security strategy is formulated through a mid-to-long-term plan or a master plan. In the past, companies established a master plan that set the direction for security and included actionable activities. However, nowadays, this is often replaced by ISMS certification or the adoption of solutions. Nevertheless, a master plan remains essential for operating a comprehensive and effective cybersecurity framework.

■ Implications

With the continuous evolution of technology, the changing patterns of criminal activity, and the shifting dynamics of international affairs, hackers are relentlessly targeting the gray zones of our organization's cybersecurity framework.

By implementing and operating security solutions, managing security frameworks, and conducting risk management, organizations can continuously defend the gray areas of cybersecurity. Furthermore, by securing visibility in emerging technological domains such as Cloud and Artificial Intelligence (AI), and by establishing and executing organizational security objectives, the cybersecurity posture of an organization can be consistently fortified against hacker attacks and incidents.

■ References

[1] Personal Information Protection Commission. “Presentation Materials from the Personal Information Policy Forum (Current Status and Response Directions of Personal Information Leakage Incidents).” Presented at the Personal Information Policy Forum, Seoul, Korea, May 21, 2025.

[2] Korea Information Security Industry Association (KISIA). Survey for Information Security Industry in Korea: Year 2024. Seoul: KISIA, October 2024.

[3] Lee, Sangkyu. “A Study on the Method for Checking the Information Security Management Level Using the Security Maturity Model.” Master’s thesis, Korea University, Graduate School of Information Security, 2019.

[4] Korea Internet & Security Agency (KISA). Introduction to the ISMS-P Certification System. Seoul: KISA, 2025.

[5] SK Shieldus. “Core Tool for Threat-Centric Security Strategy: Rule Framework.” SK Shieldus Blog, June

Keep up with Ransomware

DireWolf Ransomware Establishing Negotiation Channels for Each Victim

■ Overview

In June 2025, the number of ransomware incidents rose slightly to 505 cases, compared to 484 in May. Since April, there has been a succession of hacking incidents and operational cessations involving major ransomware groups. Conversely, there is an observable increase in the proportion of new ransomware groups that operate for brief periods of one to two months. This trend appears to be driven by heightened pressure from ongoing law enforcement crackdowns and the growing reluctance of victimized companies to pay ransoms. Consequently, ransomware groups are increasingly adopting strategies such as employing ransomware-as-a-service to conduct concentrated operations over short durations, engaging in multiple ransomware projects under a single organizational umbrella, and frequently altering their identities through rebranding.

An illustrative example supporting this trend is the official cessation of ransomware activities by the Hunters group in early July. On July 3rd, they announced on their dark web leak site, stating, "We have decided to terminate the Hunters International project." Acknowledging the impact of their actions, they declared their intention to distribute a decryption tool free of charge as a gesture of goodwill. However, the decryption tool has yet to be released, and currently, only the data of all affected companies has been removed from the dark web leak site. The movement towards terminating their project had been underway since November of the previous year. A post was uploaded to the panel used by affiliates of Hunters, indicating that while ransomware projects carry high risk, their profitability is diminishing, prompting the decision to terminate such projects. In January, they internally unveiled a new project, World Leaks, which focuses solely on data exfiltration. Subsequently, they commenced activities under World Leaks in May, and by July, they officially concluded the Hunters project.

Significant transformations continue to unfold across the entire infrastructure of cybercrime. Notably, key administrators of one of the prominent hacking forums, BreachForums, were apprehended by the French cybercrime investigation unit (BL2C) in February and June, leading to the forum's provisional shutdown. Established in 2022 as a successor to the RaidForums, which was launched in 2015, BreachForums has been under continuous surveillance by law enforcement agencies since its inception. In 2023, the administrator known as pompompurin was arrested by the FBI, resulting in the seizure of the site. Subsequently, in 2024, the arrest of another administrator, Baphomet, led to another closure. The forum was once again shut down in April 2025, when the administrators explained that a zero-day vulnerability in the open-source forum software MyBB, used by BreachForums, allowed law enforcement agencies to gain access, prompting a temporary deactivation of the forum. According to announcements, BL2C apprehended IntelBroker, a significant figure, in February of this year, followed by the arrest of four key individuals—ShinyHunters, Hollow, Noct, and Depressed—in June. This series of arrests has severely impacted the forum's operations, rendering BreachForums inactive to this day. Although other administrators hinted at a revival of BreachForums in July, no official restoration of the site has been confirmed thus far.

Amidst reports of the cessation of activities by established groups and the arrest of cybercriminals, there have been observations of other groups actively recruiting partners in preparation for their operations. The Nova group, which initially appeared under the moniker RaLord in April and underwent rebranding in May, has intensified its activities by uploading promotional content on the RAMP forum in June. They are not only advertising their affiliate services, previously promoted on their dark web leak site, but are also meticulously detailing the functionalities of their ransomware, seeking partners to utilize their ransomware services. The Chaos group, which has been active since 2021, has also commenced a robust promotional campaign. Initially operating without a dedicated dark web leak site, they began managing one in April 2025 and posted recruitment advertisements on the RAMP forum in June, seeking collaborators. Additionally, the newly emerged WarLock group also posted a recruitment notice for new partners on the RAMP forum in June; however, their dark web leak site is currently inaccessible.

As of the first half of this year, the Qilin group, which ranks second only to Clop in terms of the number of victims posted on the dark web (333 cases), has been identified as exploiting vulnerabilities in the operating system (FortiOS) of Fortinet's security equipment during ransomware attacks conducted in May and June. The vulnerabilities exploited in these attacks are the remote code execution vulnerability CVE-2024-21762 and the authentication bypass vulnerability CVE-2024-55591, both of which have already had patches released. Nevertheless, Qilin continues to target unpatched vulnerable systems in their operations. This underscores the critical importance of regularly applying patches to software and security equipment, as attackers predominantly focus on systems that have not been updated with the latest security patches.

■ Ransomware News

Hunters International Ends Ransomware Operation

- They officially announced on July 3rd they will terminate their ransomware activities through their own DLS.
- The victim companies and all data will no longer be accessible through the DLS, and free decryption tools will be provided to the victim companies.
- Internally, since January, they have been preparing to shift from the ransomware project to a data theft project.
- The project that emerged in May is called World Leaks.

BreachForums Key Figures Arrested, Operations Halted

- IntelBroker was arrested in February by the French cybercrime investigation unit (BL2C).
- In June, four key figures—ShinyHunters, Hollow, Noct, and Depressed—were additionally arrested.
- In April, BreachForums temporarily shut down the site, citing a MyBB vulnerability that allowed law enforcement access.
- Recovery was planned for July, but no official restored site has been confirmed.

Qilin Group exploiting Fortinet vulnerability

- Qilin Group exploited a FortiOS vulnerability in attacks during May and June.
- The vulnerabilities used were RCE vulnerability (CVE-2024-21762) and the authentication bypass vulnerability (CVE-2024-55591).
- Both vulnerabilities have been patched, but attacks target systems that have not yet applied the updates.

New WarLock group found Korean language in DLS source code

- The group was revealed by posting a promotional message on the Russian hacking forum RAMP.
- Since multiple victims were posted before the reveal, the group is believed to have been active before June.
- Korean comments were found in the publicly released DLS.

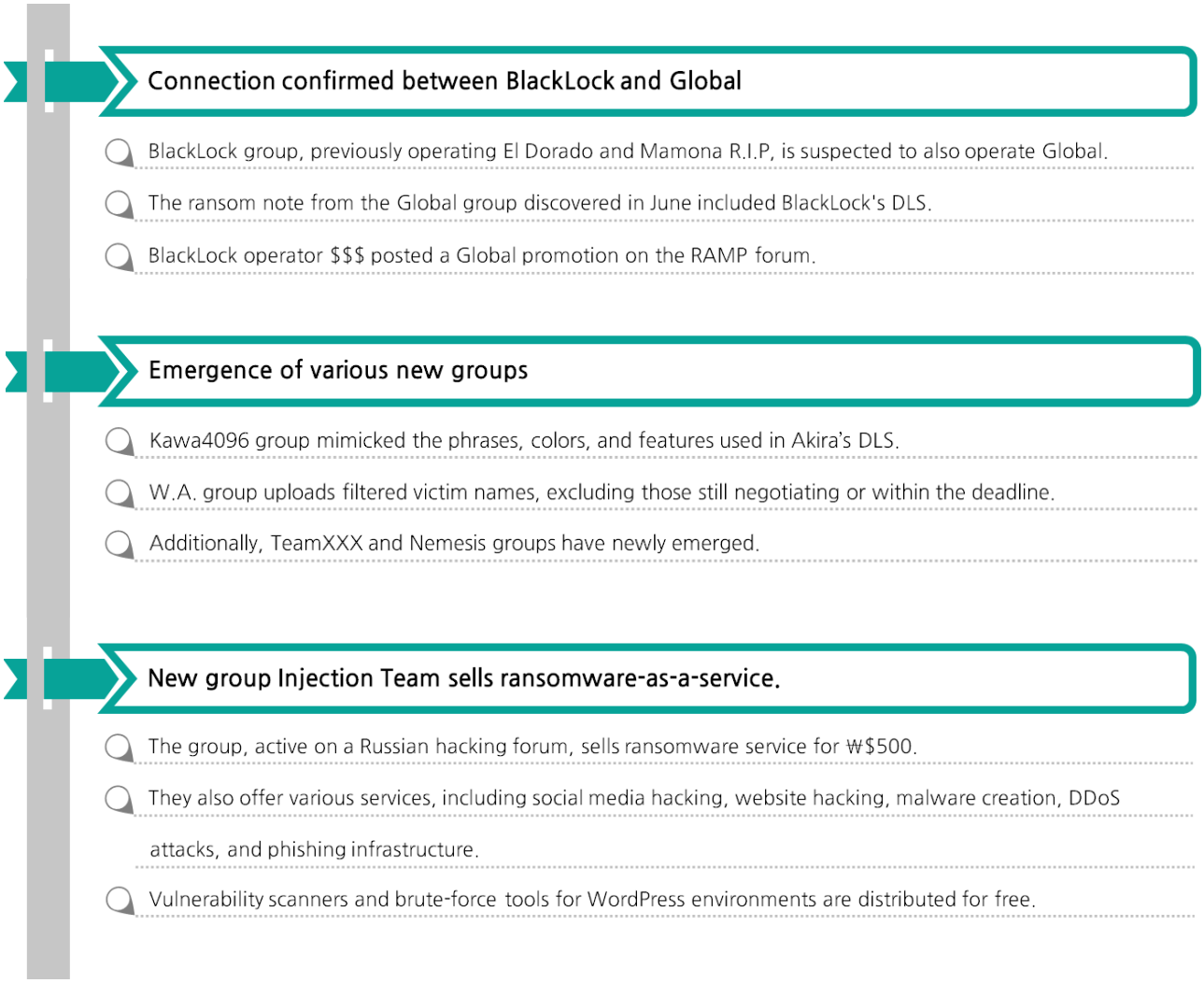


Figure 1. Ransomware Trends

■ Ransomware Threats

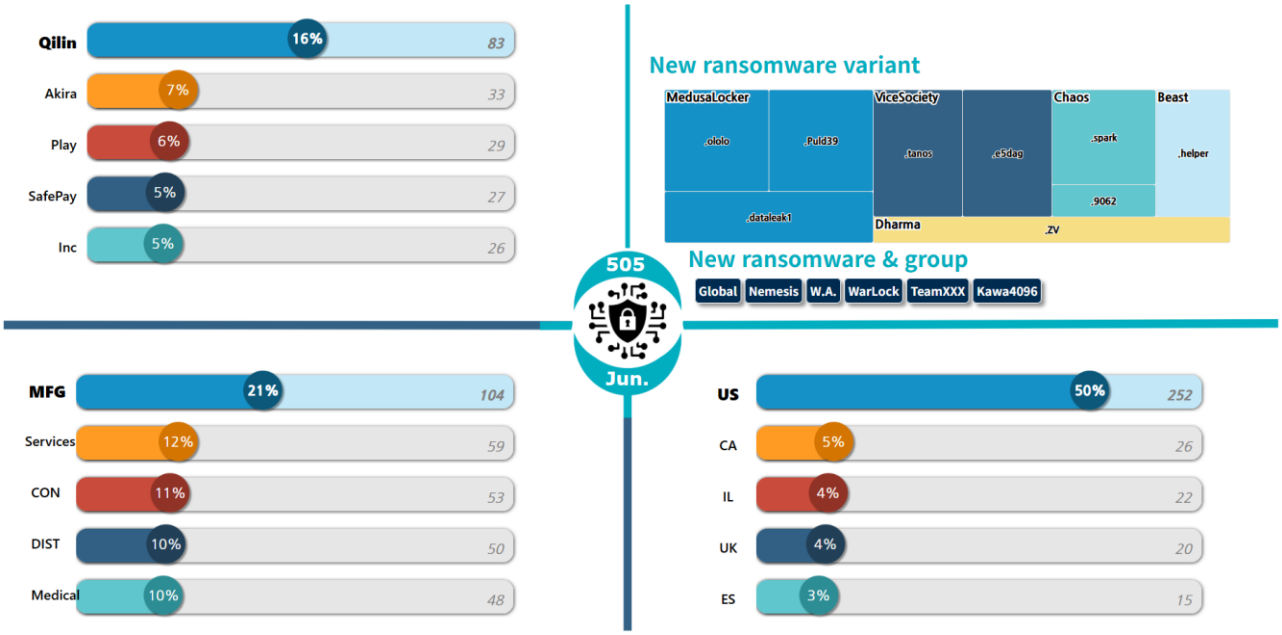


Figure 2. Status of Ransomware Threats as of June 2025

New Threats

In June, a total of five new ransomware groups emerged, with one group resuming operations following a rebranding. The newly established group, TeamXXX, reported eight victims in June, while the new group W.A. reported four. Notably, the W.A. group demonstrates a strategy of filtering and uploading the names of victimized companies that are either in the midst of negotiations or have not yet surpassed the payment deadline. Should negotiations fail or deadlines be exceeded, they proceed to disclose both the data and the names of the companies involved.

```
159             title: '!!import',
160         html: 'In order to ensure communication efficiency, please contact us via Tox; we will no longer be resp
12px;">3DCE1C43491FC92EA7D1D322040B254FDD2731DD1C2DDC2B9E819FDC946BDC3CD251FA3B694A</span><br><b>QtoxID(2)</b>:<
12px;">F79A71AD8BB2E3E7EDFC38970FDCD5E922E429B5DFC325C7D0E91F216DE8F3537C1A1C97F197</span>',
161         icon: 'info',
162             confirmButtonText: 'ok'
163         });
164         // 클라이언트 데이터 로드 함수
165         async function loadClients() {
166             console.log("loadClients called");
```

Figure 3. Source Code of WarLock DLS Page

The newly identified group, WarLock, was discovered when a user presumed to be an operator, identified as cnkjasdfgd, uploaded a promotional post on the Russian hacking forum RAMP. It is surmised that their actual activities commenced prior to June, as multiple victims have already been listed on dark web leak sites. Furthermore, the source code on these dark web leak sites contained annotations in Korean; however, these sites have since been shut down and are currently inaccessible.

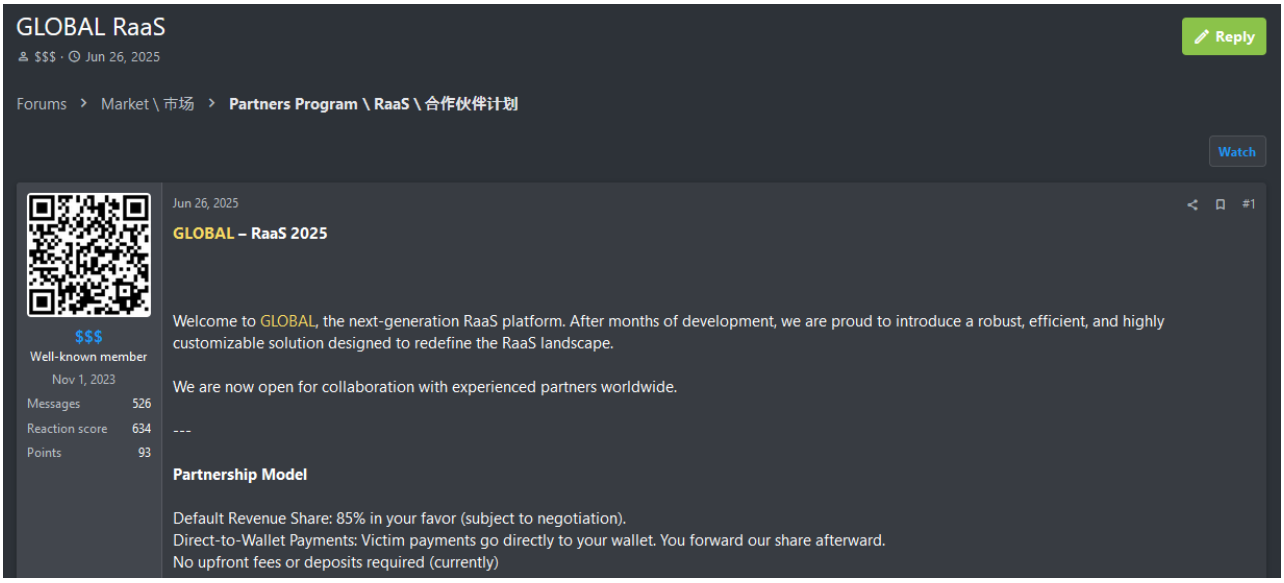


Figure 4. Global RaaS Promotional Material

The newly identified Global group has been confirmed to have affiliations with BlackLock. Initially, in early June, a version of the Global ransomware was discovered that was almost identical to Mamona ransomware, another project attributed to BlackLock. According to the ransom note associated with this ransomware, the perpetrators referred to themselves as Global; however, the note included the URL of BlackLock's dark web leak site. Furthermore, during negotiation chats, it was mentioned that the victims could verify the breach on Global group's dark web leak site. Around the same time, the operator of BlackLock, known as $$$, altered the promotional content and profile on RAMP, changing the name from BlackLock to Global BlackLock. By the end of June, $$$ had uploaded promotional material directly endorsing Global RaaS, thereby substantiating the connection between BlackLock and Global.

Figure 5. Nemesis Negotiation Page

The Nemesis group has yet to reveal a dedicated webpage for disclosing exfiltrated data. Unlike other groups that either maintain a mere negotiation chat page or consolidate victim and leaked data information on a single platform, Nemesis directs victims to a dark web page via a ransom note, which includes a unique token for each victim. Subsequently, they display samples of the data they have exfiltrated and provide both the demanded ransom amount and a messenger ID for negotiation purposes.

Figure 6. Dark Web Leak Sites (Top: Akira, Bottom: Kawa4096)

The newly identified Kawa4096 group's dark web leak site exhibits a design strikingly similar to that of the Akira group's dark web leak site. This resemblance extends beyond mere aesthetics, encompassing the specific phrases and color schemes employed, as well as the interactive interface that mimics a console window, wherein users must input commands to access additional data. However, despite these similarities, it is not uncommon for dark web leak sites to imitate the design or phrasing of others, even in the absence of a direct relationship or connection between the groups. Therefore, it is imperative to continue monitoring the potential affiliations between these two entities.

Top 5 Ransomware

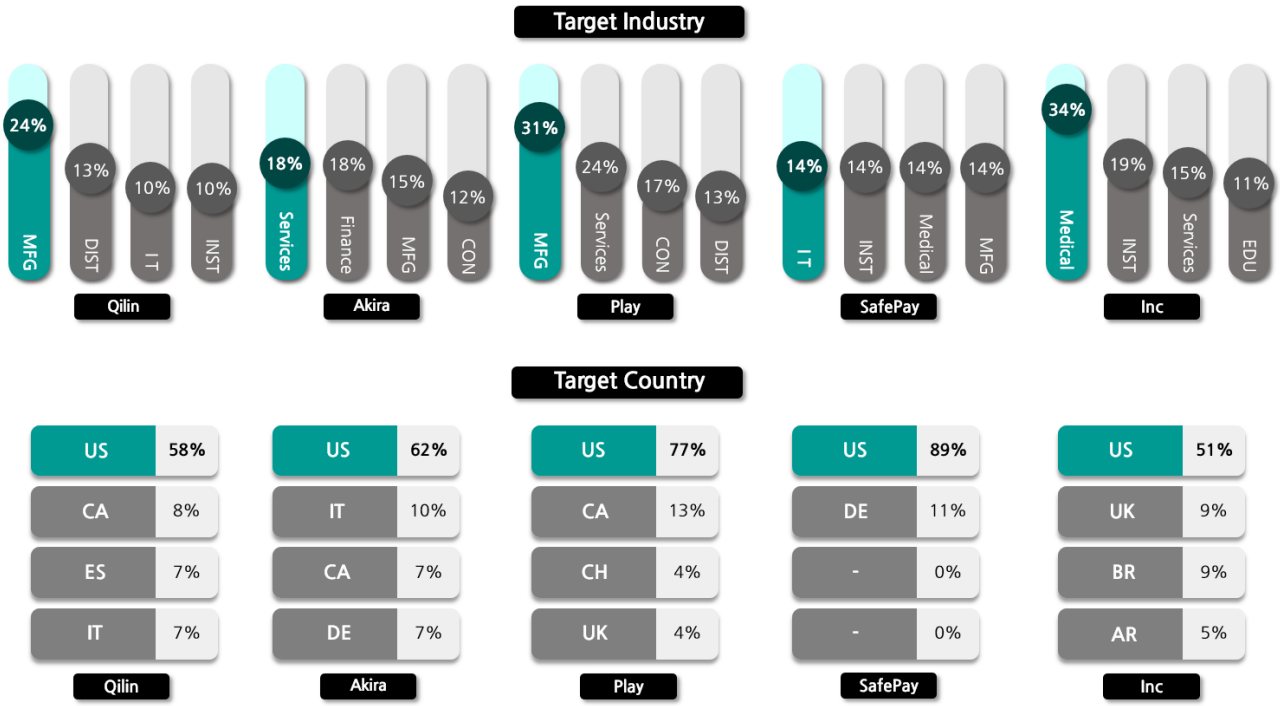


Figure 7. Overview of Major Ransomware Attacks by Industry/Country

On June 24, the Qilin group launched a cyberattack on Covenant Health, a healthcare institution in the United States, resulting in the exfiltration of internal documents. The compromised data encompassed patient medical information, contracts, tax documents, and files capable of identifying employees. Furthermore, on June 23, the American logistics company Estes Forwarding Worldwide fell victim to an attack, with samples such as passport scans, driver's licenses, and employee information spreadsheets being posted on the dark web. Similarly, the British spring manufacturing company Airedale Springs Ltd. was targeted in an attack towards the end of June, leading to the partial exposure of internal operational documents and supply chain-related materials.

In early June, the Akira group launched an attack on the Sleepy Hollow Country Club, a social club in the United States, exfiltrating approximately 14GB of internal data. By the end of June, they had disclosed all the data, which encompassed not only personal information such as employees' passports and social security numbers but also contracts and financial statements. Furthermore, they targeted the outsourcing firm Datrose, seizing around 5GB of data. This dataset was confirmed to contain personal information, including emails and addresses, as well as non-disclosure agreements and financial statements.

The Play group launched an attack on S&H Express, a transportation company based in Pennsylvania, USA, resulting in the exfiltration of data. The leaked samples included contracts, employment-related documents, tax files, and copies of driver's licenses. Additionally, on June 27, Cartel Communication Systems, a Canadian telecommunications equipment distribution company, was also targeted. This breach led to the exposure of customer lists, internal project documents, supplier contracts, and certain technical documents on the dark web.

The SafePay group orchestrated a cyberattack on the Liberty Township School District in Ohio, USA, resulting in the exfiltration of 48GB of data encompassing internal financial records, operational documents, and personnel-related files. Furthermore, the German IT service provider MCSL GmbH fell victim to a similar breach, leading to the exposure of client reports, project documentation, and internal communication files. Additionally, The Overhead Door Company, an American garage door manufacturer, was compromised, with internal materials such as technical documentation, accounting records, and employment contracts being disclosed.

The Inc group has claimed responsibility for exfiltrating approximately 3.5TB of data from the German telecommunications equipment manufacturer, funktel GmbH. As evidence, they have released samples of various documents, including blueprints of major products, internal emails, payroll statements, and operational plans. Furthermore, they have targeted the American healthcare provider, Medical Center of Marin, resulting in the breach of patient information. This includes questionnaires containing personal data, medical reports, and patient identification documents.

■ Focus on Ransomware

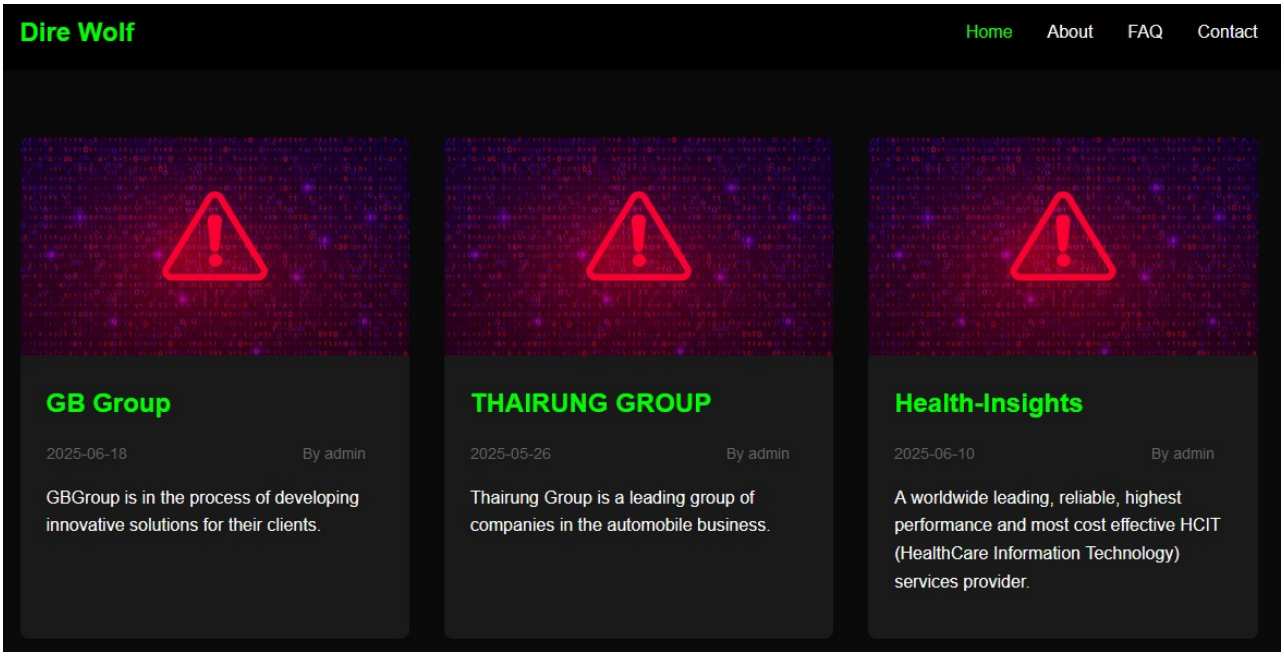


Figure 8. DireWolf Dark Web Leak Site

Since commencing operations in May 2025, the DireWolf group has publicly disclosed a total of 16 victims. For each victim, they meticulously document which files were exfiltrated and the exact date of upload. Should negotiations fail or a predetermined period elapse, they proceed to publish the data on the dark web, making it accessible to all users.

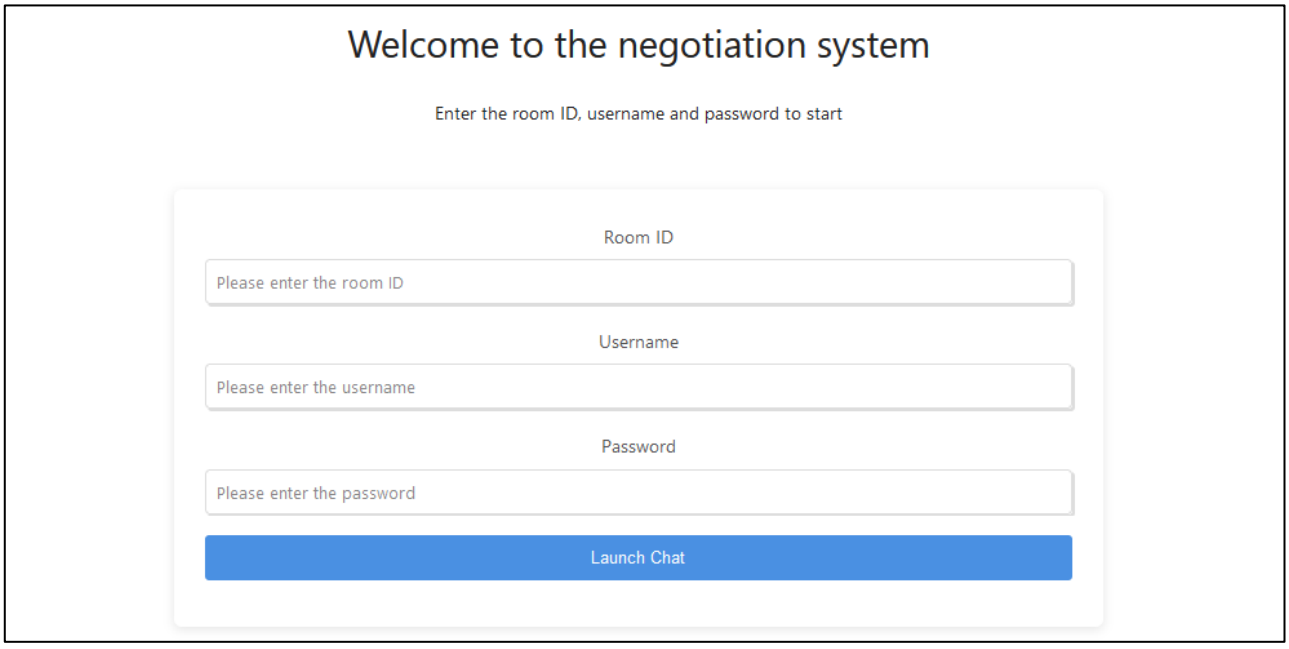


Figure 9. DireWolf Dark Web Negotiation Page

The ransom note not only provides the address of the aforementioned dark web leak site but also includes the address of a dark web chat site for negotiations, along with the necessary Room ID, Username, and Password for access. Furthermore, instead of uploading sample data to the dark web to prove their data exfiltration, the perpetrators compress the data and upload it to the cloud storage service GoFile, attaching the link in the ransom note so that only the victim can verify it.

Given the provision of a cloud link containing sample data and the dissemination of information required to access the negotiation page, it is highly probable that the perpetrators are deploying a modified version of ransomware tailored to each individual victim. They may simply alter the content of the ransom note before distribution, and it is also plausible that they are customizing other functionalities prior to dissemination. At present, ransomware targeting a single victim has been identified, and the analysis of this instance is being shared to facilitate preparedness against impending ransomware threats.

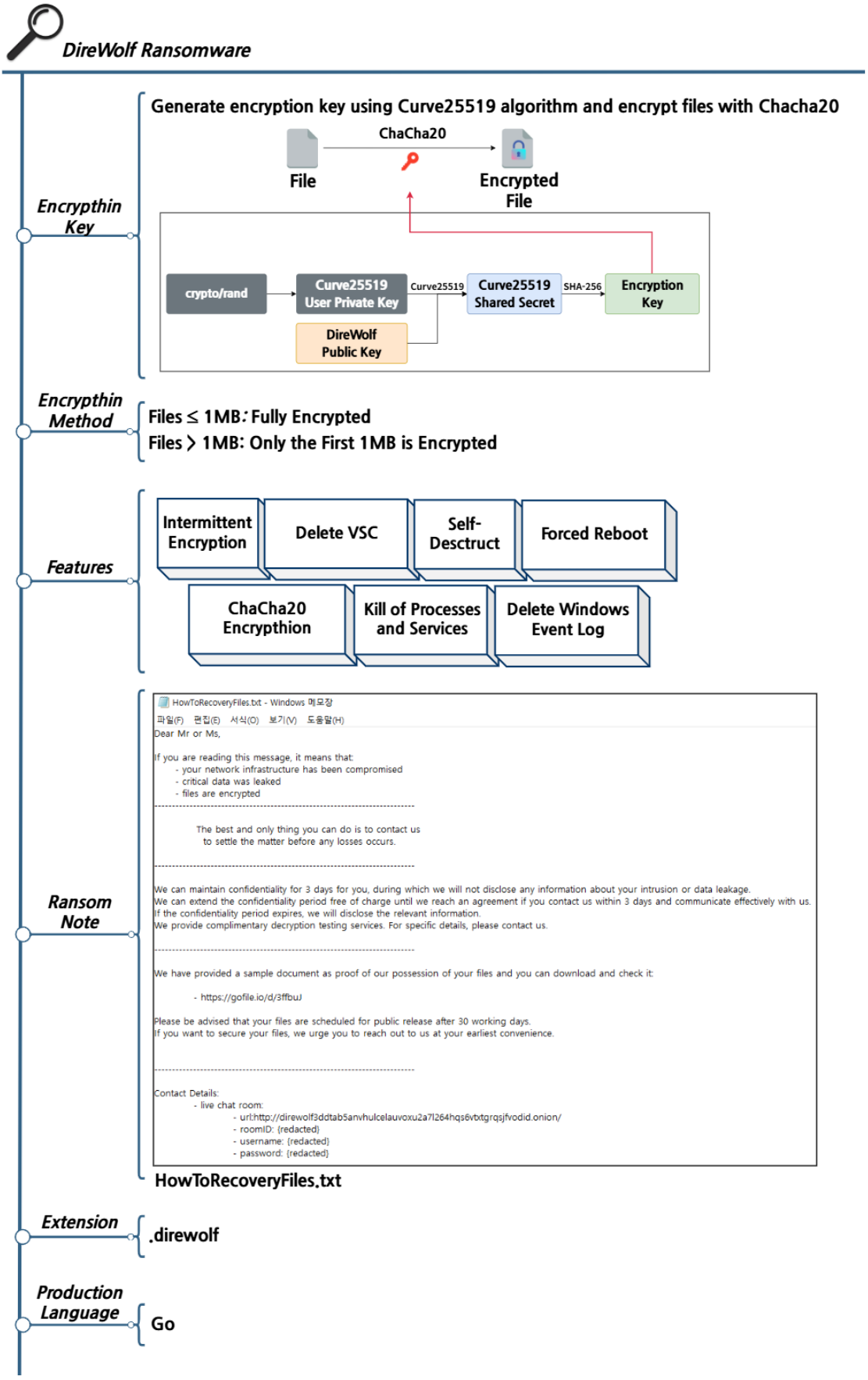


Figure 10. Overview of DireWolf Ransomware

DireWolf Ransomware Strategy

Figure 11. DireWolf Ransomware Attack Strategy

DireWolf does not utilize a separate configuration file; instead, it operates through the use of two command-line arguments to control its functionalities. By employing the -h argument, users can access a description of these command-line parameters, while the -d argument allows for the encryption to be confined to a specific directory.

Options	Description
-h	Display usage/help information
-d <path>	Encrypt only the specified path

Table 1. DireWolf Execution Parameters

DireWolf employs a mutex to prevent redundant execution. Upon initiation, the ransomware creates a mutex named "Global\direwolfAppMutex," which it releases just before termination. If an identical mutex is already present, it indicates that the same ransomware is currently active, prompting the termination of the current process to avert duplicate execution. Furthermore, DireWolf ransomware generates an empty file at the path C:\runfinish.exe after encrypting the target system. At the commencement of the ransomware, it checks for the existence of this file to prevent redundant scanning and encryption of an already encrypted system. Should the mutex or the runfinish.exe file be detected, the ransomware not only terminates but also proceeds with self-deletion using the command below.

```
cmd /C timeout /T 3 & del /f /q <path> & exit
```

Table 2. Self-Deletion Commands

In addition to self-deletion, various logs and traces are erased to prevent recovery, hinder analysis, and evade detection. The process of the running Windows event log is terminated, and the default event logs within the Windows environment are deleted. Furthermore, utilizing the command prompt, backup copies are deleted, and both the deactivation of the recovery environment and the prevention of entry into recovery mode are executed.

Command	Description
Get-WmiObject -Class win32_service -Filter "name = 'eventlog'" | select -exp ProcessId exp ProcessId	Check event log PID
Get-WmiObject -Class win32_service -Filter "name = 'eventlog'" | select -exp ProcessId	Check event log PID
taskkill /f /pid <PID>	Kill event log process
vssadmin delete shadows /all /quiet	Delete restore point
wmic shadowcopy delete /nointeractive	Delete restore point
wbadmin stop job -quiet	Abort executing backup
wbadmin disable backup -quiet	Cancel scheduled backup
wbadmin delete backup -keepVersions:0 -quiet	Delete All backups
wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0 -quiet	Delete system state backup
wbadmin delete catalog -quiet	Delete metadata of backup
bcdedit /set {default} recoveryenabled No	Disable WinRE
bcdedit /set {default} bootstatuspolicy ignoreallfailures	Black access to recovery
wevtutil cl Application	Clear Application log
wevtutil cl system	Clear System log
wevtutil cl security	Clear Security log
wevtutil cl setup	Clear Setup log

Table 3. Commands for Backup and Event Log Deletion

To facilitate seamless file encryption, specific processes and services are prioritized for termination. The processes and services targeted for termination are detailed in the table below.

Processes
wxServerView.exe, sqlmangr.exe, RAgui.exe, supervise.exe, Culture.exe, Defwatch.exe, httpd.exe, wsa_service.exe, synctime.exe, vxmon.exe, sqlbrowser.exe, memtas.exe, tomcat6.exe, Sqlservr.exe, agntsvc.exe, dbeng50.exe, dbsnmp.exe, dbsrv12.exe, encsvc.exe, excel.exe, firefox.exe, vss.exe, infopath.exe, isqlplussvc.exe, msaccess.exe, mspub.exe, mydesktopqos.exe, mydesktopservice.exe, ocautoupds.exe, ocomm.exe, ocssd.exe, onenote.exe, oracle.exe, outlook.exe, powerpnt.exe, sqbcoreservice.exe, sql.exe, steam.exe, tbirdconfig.exe, thebat.exe, thunderbird.exe, visio.exe, WinSAT.exe, winword.exe, wordpad.exe, onedrive.exe, wrapper.exe, xfssvccon.exe, sqlservr.exe, sqlagent.exe, sqlwriter.exe, MSExchangeIS.exe, MSExchangeTransport.exe, MSExchangeMailboxAssistants.exe, MSExchangeRepl.exe, MSExchangeRPC.exe, MSExchangeServiceHost.exe, notepad++.exe, notepad.exe

Table 4. Target Processes for Termination

Services
AcrSch2Svc, backup, BackupExecAgentAccelerator, BackupExecAgentBrowser, BackupExecDiveciMediaService, BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, BackupExecVSSProvider, CAARCUpdateSvc, CASAD2DWebSvc, ccEvtMgr, ccSetMgr, DefWatch, GxBlr, GxCIMgr, GxCVD, GxFWD, wuauserv, GxVss, Intuit.QuickBooks.FCS, memtas, mepocs, PDVFSService, QBCFMonitorService, QBFCService, QBIDPService, RTVscan, SavRoam, sophos, sql, stc_raw_agent, veeam, VeeamDeploymentService, VeeamNFSSvc, VeeamTransportSvc, VSNAPVSS, vss, YooBackup, YooIT, zhudongfangyu, SQLPBDMS, SQLPBENGINE, MSSQLFDLauncher, SQLSERVERAGENT, MSSQLServerOLAPService, SSASTELEMETRY, SQLBrowser, SQLServerDistributedReplayClient, SQLServerDistributedReplayController, MsDtsServer150, SSISTELEMETRY150, SSISScaleOutMaster150, SSISScaleOutWorker150, MSSQLLaunchpad, SQLWriter, SQLTELEMETRY, MSSQLSERVER, BackExecRPCService, bedbg, Culserver, dbeng8, MSExchange, msftesql-Exchange, msmdsrv, MSSQL, sqladhlp, SQLADHLP, sqlagent, SQLAgent, SQLAgent$SHAREPOINT, tomcat6, vmware-converter, vmware-usbarbitator64, WSBExchange

Table 5. Services Scheduled for Termination

After terminating the target services and processes, encryption is initiated. By utilizing the -d parameter, encryption is confined to a specific directory and its subdirectories. In the absence of the -d parameter, all connected drives, with the exception of CD/ROMs, are encrypted. Once the encryption targets have been designated, each directory is traversed to ascertain whether it qualifies as an exception item, and a ransom note is generated accordingly. The encryption exception targets are outlined in the table below.

Directory names	Extensions and File names
AppData, Boot, C:\Windows, SYSVOL, Tor Browser, Internet Explorer, Google, Opera, Opera Software, Mozilla, Mozilla Firefox, $Recycle.Bin, ProgramData, All Users, bootmgr, system volume information, inte, msocache, perflogs, ntldr, Program Files, Program Files (x86), #recycle, $windows.~bt, ntuser.dat, NTUSER.DAT	HowToRecoveryFiles.txt, .exe, .dll, .sys, .drv, .bin, .tmp, .iso, .img, .direwolf

Table 6. Subjects Exempted from Encryption

File encryption is categorized into full encryption and partial encryption based on the file size. Files that are 1MB or smaller undergo full encryption, whereas files exceeding 1MB have only their first 1MB encrypted. For each encryption target, a random private key is generated, and a Curve25519 shared secret is created using the hardcoded public key of DireWolf, which is then utilized for encryption. This shared secret is hashed using the SHA-256 algorithm to serve as the encryption key. The key is subsequently hashed again with SHA-256, and a portion of this hash is employed as a nonce to encrypt the file using the ChaCha20 algorithm. At the end of the file, the Curve25519 public key necessary for key recovery is stored alongside a 6-byte segment of arbitrary data (0xAB 0xBC 0xCD 0xDE 0xEF 0xF0).

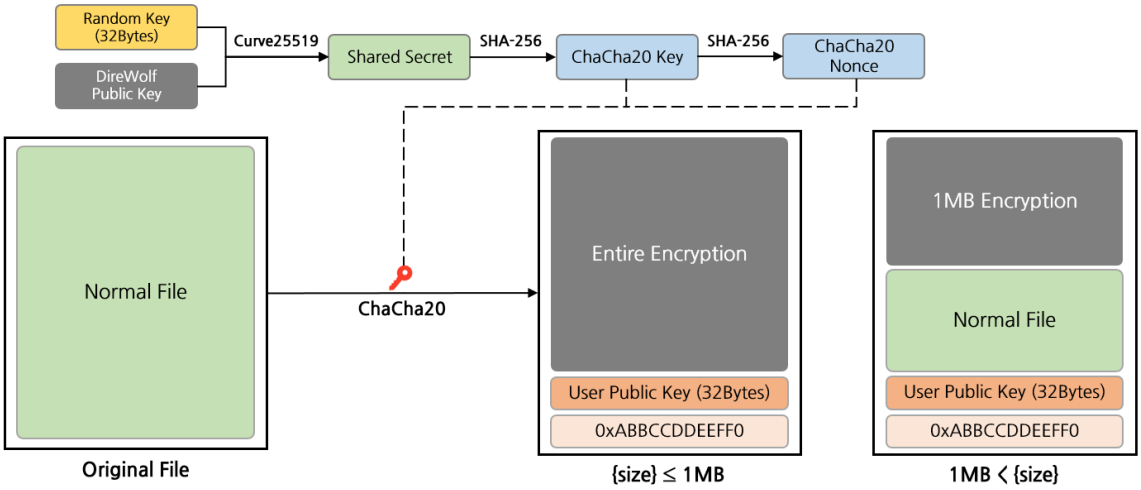


Figure 12. File Encryption Method

Upon the completion of file encryption, an empty file is generated at the path C:\runfinish.exe, and a reboot is attempted after a 10-second interval. Should the reboot attempt fail, the system proceeds with self-deletion before terminating the process. Conversely, if the reboot is successful, the self-deletion process is not executed. The command used for rebooting is detailed in the table below.

cmd /c start shutdown -r -f -t 10

Table 7. Reboot Commands

Response Strategies for DireWolf Ransomware

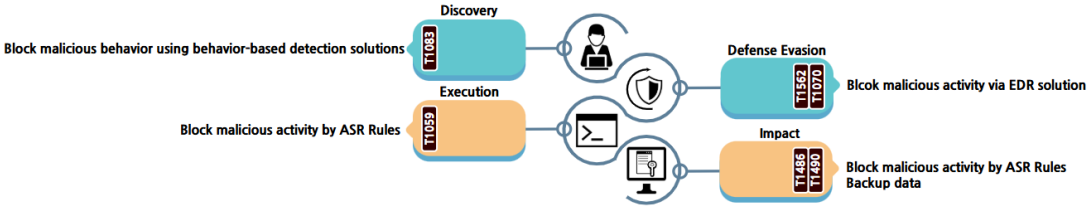


Figure 13. Countermeasures Against DireWolf Ransomware

The DireWolf ransomware creates an empty file named runfinish.exe upon termination to prevent redundant execution. During its execution, it checks for the presence of this file on the system to avoid encrypting the same system multiple times. Since it inspects files in specific paths, behavior-based detection solutions can be employed to identify and block such malicious activities.

To evade detection of malicious activities, the process of event logging is halted, and the default event logs in Windows are deleted. By employing an Endpoint Detection and Response (EDR) solution, it is possible to thwart malicious activities such as the deactivation of specific processes or the deletion of event logs. Furthermore, there exists a self-deletion feature designed to prevent analysis, which can also be counteracted by utilizing an EDR solution to block such malicious actions.

Furthermore, the aforementioned malicious activities of the DireWolf ransomware are executed utilizing the Windows Command Prompt. Consequently, by activating Attack Surface Reduction (ASR) rules, it is possible to intercept and prevent these anomalous processes, thereby thwarting malicious actions. To further inhibit users from arbitrarily recovering encrypted files, the ransomware employs a total of nine commands to obliterate all backup copies present on the system and disable recovery options. Activation of ASR rules not only obstructs file encryption but also prevents the deletion of backup copies. Additionally, it is imperative to implement measures such as dispersing backup copies to separate networks or storage facilities, ensuring that recovery remains feasible even if the system undergoes encryption.

Indicators of Compromise (IoCs)

Hash(SHA-256)
8fdee53152ec985ffeeeda3d7a85852eb5c9902d2d480449421b4939b1904aad
27d90611f005db3a25a4211cf8f69fb46097c6c374905d7207b30e87d296e1b3
b6fa7a34b57803d2b80f3f484656d34997231597b6c1aa7fc8a386d6474c8afe

■ Reference Websites

• Group-IB (https://www.group-ib.com/blog/hunters-international-ransomware-group/)

• LE Parisien (https://www.leparisien.fr/high-tech/la-police-interpelle-cinq-hackers-francais-de-haut-vol-derriere-un-celebre-forum-de-vol-de-donnees-25-06-2025-QJTPFTDPQZAP7B25MF24YLHU6E.php)

• BleepingComputer (https://www.bleepingcomputer.com/news/security/critical-fortinet-flaws-now-exploited-in-qilin-ransomware-attacks/)

Special Report

Zero Trust Security Strategy: Network

Byung-gwon Hwang, SK Shieldus

■ Overview of the Network Pillar

The network serves as the foundational backbone of all IT infrastructure, acting as the pivotal conduit that interlinks an organization's data, systems, users, and devices within a zero-trust environment. Every digital activity we engage in—be it email communication, web services, file sharing, cloud operations, or remote access—transpires through the medium of the network. The notion that the network 'connects everything' inherently signifies that the majority of security threats confronting an organization are propagated via the network.

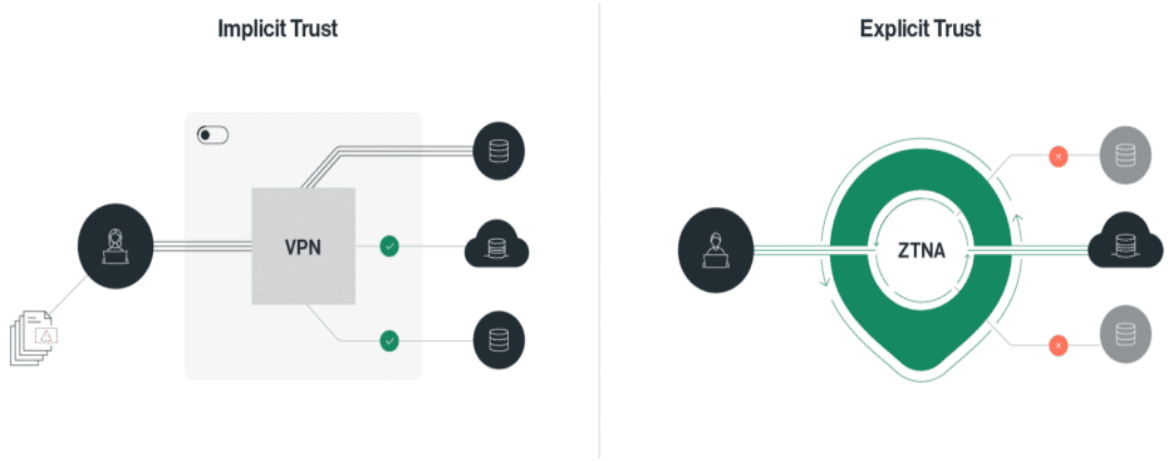
In contemporary cybersecurity landscapes, the majority of attacks, including actual breaches, ransomware, phishing, and data exfiltration, are rarely executed without traversing through networks. Adversaries relentlessly exploit vulnerabilities within networks, such as unauthorized access, internal traffic obfuscation, encryption circumvention, and inadequately segmented access policies. Recently, there has been a burgeoning trade on the dark web and similar platforms involving tangible network attack infrastructures. These include exploits for network penetration, VPN/proxy accounts, tools for circumventing network segmentation, and decryption utilities for encrypted traffic.

The traditional perimeter-based security model was predicated on the division of networks into trusted internal zones and untrusted external zones, with a primary focus on perimeter defense. However, with the rapid diversification of network environments, driven by factors such as the proliferation of cloud computing and the rise of remote and telecommuting work, this conventional perimeter security model has revealed significant limitations. It has struggled to detect threats that have infiltrated the perimeter or to control threats propagating internally. Furthermore, it has consistently failed to effectively prevent lateral movement within the network during security breaches.

In the domestic context, the traditional security infrastructure, primarily designed around physical network segregation, is increasingly becoming a structural constraint due to the expansion of remote and flexible working arrangements. To address these challenges, initiatives such as the National Intelligence Service-led 'National Network Security Framework Guidelines (N2SF)' and the Financial Services Commission's 'Roadmap for Improving Network Segregation in the Financial Sector' are currently advocating for a phased relaxation of network segregation environments, coupled with the implementation of zero-trust-based compensatory measures. It is imperative that these considerations are thoroughly integrated when designing a zero-trust-based network architecture.

As an alternative solution to address these issues, Zero Trust Network Access (ZTNA) has emerged. ZTNA operates on the principle of never inherently trusting any user or device requesting network access, instead consistently verifying them. Regardless of whether the network is internal or external, every access request is evaluated in real-time through a multifaceted assessment of the user's identity, the security status of the device, and the access context, which includes factors such as location, time, and behavioral patterns. Only after this rigorous verification process are authenticated users and devices granted resource access, strictly adhering to the principle of least privilege.

Unlike traditional perimeter-based models such as VPNs, the Zero Trust Network Access (ZTNA) approach continuously evaluates and verifies the trustworthiness of users and devices even when accessing internal networks. Traditional perimeter security methods like VPNs are predicated on the concept of 'Implicit Trust,' which, upon a single network connection, permits extensive access to most internal resources. In stark contrast, ZTNA employs an 'Explicit Trust' model, wherein the trustworthiness of users and devices is explicitly verified at every moment. Through this approach, organizations can fundamentally prevent the proliferation of threats that have infiltrated the internal network, significantly enhancing both the speed and accuracy of threat response through meticulous and dynamic access control.



* Source: Cato Networks, "Zero Trust Network Access (ZTNA)"

Figure 1. Perimeter-Based Security Model vs. Zero Trust Network Access (ZTNA) Model

In a Zero Trust architecture, the network pillar transcends its role as a mere conduit for connectivity, undertaking a pivotal function in the tangible management of organizational security and the continuous detection and interception of threats. This transformation is perpetually evolving in tandem with the escalating complexity of network environments, enabling organizations to establish a more robust and adaptable security framework.

■ Key Elements of the Network Pillar

The network pillar, given the structural characteristic that all IT assets and services are interconnected through the network, stands as the critical pillar where technical controls and actual security measures must be most intensively applied within a zero trust architecture environment. The network serves as the foundation connecting all elements within an organization, including data, systems, users, and devices, and is the primary conduit through which security threats predominantly manifest. Therefore, it operates as the most crucial domain for implementing the principles of zero trust in a practical manner.

In a zero-trust environment, the demarcation between internal and external networks is rendered obsolete, with all traffic, sessions, and connections being perceived as potential threats. This paradigm necessitates the acquisition of real-time visibility over network flows and the implementation of dynamic and granular policy enforcement. To achieve this, an integrated operation of various managerial and technical components is imperative, including network inventory, flow analysis, traffic encryption, network access control, logical boundary configuration, segmentation, network flexibility and resilience, as well as visibility and monitoring.

Below is a summary of the key components of network pillars and the specific management and technical strategies for their implementation, analyzed from the perspective of Zero Trust maturity.

1. Network Inventory

In a Zero Trust environment, the network inventory serves as the foundational point for systematically identifying and managing the status of diverse communication infrastructures within the organization. This encompasses all wired and wireless networks, cloud services, and internet access, as well as the physical and logical network devices that constitute these infrastructures, such as switches, routers, wireless access points, firewalls, and SDN/SDP equipment. The scope of management extends beyond traditional on-premises network devices to include virtual network devices residing in cloud environments and network devices located in remote areas.

The crux of network inventory management lies in the precise identification of all assets that transmit and receive data across the network, ensuring that information remains current throughout the entire lifecycle of the equipment, including its acquisition, modification, transfer, and disposal. To achieve this, organizations must systematically integrate and manage data concerning the inventory of network equipment, key attributes such as MAC addresses, IP addresses, operating systems, and hardware specifications, as well as their intended use, installation locations, and owning departments, in conjunction with asset management systems and network monitoring tools.

Network equipment can be categorized and managed according to their purpose and role (e.g., enterprise network, internet network, cloud network). Furthermore, this group information must be automatically updated in response to changes in the equipment's status, such as new installations, repurposing, or relocation. Differentiated policies can be applied to each group, and they can be utilized in conjunction with network segmentation and access control.

A network inventory transcends mere list management, encompassing both the logical and physical architectures of network infrastructures. Diverse network domains within an organization, such as the operational network, internet network, and cloud network, must be distinctly delineated. Each network domain should have its equipment, connection structures, traffic flows, and security policies systematically managed. These network definitions serve as technical benchmarks when implementing next-generation network architectures, such as Software-Defined Networking (SDN), Software-Defined Perimeter (SDP), and network segmentation.

In organizations with a high level of maturity, all network resources are automatically registered in the asset management system upon introduction. Furthermore, whenever network changes occur, these resources are integrated with a unified monitoring system to provide real-time topology information, thereby ensuring visibility into the status and modifications of network equipment. Consequently, the organization can effectively implement a variety of network security and operational policies, such as network access control, anomaly detection, and incident response, based on the network inventory.

2. Network Flow Analysis

In a Zero Trust environment, network flow analysis constitutes a pivotal security activity that involves real-time monitoring of all traffic and connection information traversing the organization's network. This process is instrumental in detecting and analyzing traffic patterns and anomalous behaviors. It has become an indispensable procedure for the early identification of threats or unauthorized access via the network, enabling prompt and effective responses.

The initial step in analyzing network flow involves precisely identifying the traffic pathways across the entire network, key connection points, and the communication flow between internal and external entities. This also includes establishing a baseline for normal traffic within distinct network domains such as business networks, internet networks, and cloud networks. Organizations must systematically collect and analyze packet flows, connection statuses, data transmission volumes, and primary communication targets by leveraging network monitoring systems and traffic analysis tools.

In this process, it is imperative to concurrently undertake periodic updates and visualizations of network routing and architecture. This should be integrated with the potential implementation of logical boundaries such as network segmentation, Software-Defined Networking (SDN), and Software-Defined Perimeter (SDP), thereby enabling a comprehensive management of the entire network structure and flow. Information pertaining to network routing and architecture serves as foundational data for various network security operations, including policy-based network access control, anomaly traffic detection, and incident response.

Securing real-time network flow visibility through the integration with a unified monitoring system via network flow analysis constitutes a pivotal requirement in a zero-trust environment. Organizations with a high level of maturity are capable of automatically detecting changes across the network, such as alterations in network connections, anomalies in flow, and modifications in routing structures. These organizations can swiftly incorporate the analysis results into their network security policies, thereby enhancing their security posture.

3. Encryption of Network Traffic

In a zero-trust environment, the encryption of network traffic is an indispensable element to ensure the confidentiality and integrity of data transmission across all network segments, irrespective of internal or external distinctions. The majority of traffic traversing the network is based on traditional protocols such as TCP and UDP. By employing standard encryption protocols like TLS and DTLS, the traffic itself is encrypted, thereby safeguarding data from a myriad of threats, including man-in-the-middle attacks, packet interception, and traffic tampering. Particularly, traffic traversing critical segments or carrying sensitive information must be protected in strict accordance with encryption policies. In the event that vulnerabilities are discovered within the encryption protocols themselves, an immediate patch and response mechanism must be established separately to address such issues.

Encryption of DNS traffic is an area that unequivocally demands attention. Originally, DNS was not designed with security in mind, rendering it susceptible to a myriad of vulnerabilities such as spoofing, Denial of Service (DOS), and man-in-the-middle attacks. Consequently, encryption technologies are being implemented, including digital signature-based protocols like DNSSEC, as well as DNS over HTTPS (DOH) and DNS over TLS (DOT), which are based on HTTPS/TLS. It is imperative to proactively devise strategies to address potential issues such as performance degradation, management complexity, and compatibility challenges arising from encryption. Notably, the DOT protocol is recommended for its superior performance and management efficiency. There is a discernible trend towards the comprehensive application of encryption across DNS traffic.

In a Zero Trust environment, it is imperative to encrypt not only TCP/UDP traffic but also other network traffic such as ICMP and SCTP. Protocols like ICMP, which inherently lack encryption capabilities, can be secured using additional security technologies such as IPSEC. Meanwhile, SCTP can leverage encryption technologies like DTLS. Furthermore, it is essential to design the network architecture to ensure that all traffic, both internal and external, is securely protected through various methods such as SSL VPN tunneling and traffic encapsulation. Additionally, it is crucial to integrate these encryption policies and their implementation status with monitoring and log analysis systems to maintain real-time visibility.

In recent developments, efforts have been made to overcome the limitations of traditional encryption methods by applying quantum cryptography technologies to network encryption channels, such as VPN tunneling. By utilizing Quantum Key Distribution (QKD) technology, it is possible to integrate quantum random number-based encryption keys into existing VPN communications. Theoretically, this approach promises enhanced security resilience against man-in-the-middle attacks and potential future threats posed by quantum computing-based hacking. However, at present, these quantum cryptography-based network encryption technologies remain largely confined to certain empirical projects and pilot programs. Instances of their commercialization and comprehensive implementation in actual organizational environments and current operational workflows are still relatively uncommon.

4. Network Access Management

In a zero-trust environment, network access management serves as a pivotal domain that meticulously regulates access to all network resources within an organization. By implementing real-time authentication, authorization, and monitoring, it maximizes the security posture against both internal and external threats. Network access management is comprised of network access control, authentication, authorization, and authentication integration, with each phase being interlinked to enhance the reliability and visibility of the organization's entire network infrastructure.

Network access control meticulously delineates access policies to network resources through an array of security apparatus such as firewalls, Network Access Control (NAC), and Intrusion Prevention Systems (IPS), while simultaneously regulating sessions and traffic within the network in real-time. In recent developments, technologies such as Software Defined Perimeter (SDP) and Micro Segmentation have been employed to logically refine network access pathways. These technologies dynamically apply granular access policies based on the trustworthiness, location, and behavioral information of users or devices. When integrated with Identity, Credential, and Access Management (ICAM) systems, it becomes feasible to comprehensively monitor and block even Bring Your Own Device (BYOD) or external devices, as well as high-risk network access sessions.

Network access authentication transcends mere device-based verification by integrating with account management systems such as Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and Identity and Access Management (IAM), as well as Single Sign-On (SSO) and Multi-Factor Authentication (MFA). This integration ensures that both the user's identity and device information are meticulously verified when accessing network resources. In the domains of Software-Defined Perimeter (SDP) and Micro Segmentation, more stringent authentication and authorization policies are enforced. These policies are complemented by real-time behavioral analysis, risk-based authentication, and additional verification measures, thereby enhancing the security framework.

Network access authorization is a procedure that meticulously manages which network resources authenticated users and devices can access, specifying the time, location, and permissions involved. Authorization policies incorporate a variety of contextual information, such as time, location, user roles, and access history. These policies are integrated with systems like Identity, Credential, and Access Management (ICAM) and unified monitoring systems to continuously assess network authorization sessions. This integration ensures that in the event of any anomalous activity, sessions can be automatically terminated or re-authenticated. The outcomes of vulnerability management can be directly applied to the risk assessment of devices. Devices that repeatedly exhibit vulnerabilities or remain unaddressed can be subjected to measures such as restricted access to sensitive data, additional authentication requirements, or network isolation, thereby effectively mitigating actual risks.

The integration of network access authentication seamlessly manages the entire network access process across all network environments within an organization, including wired, wireless, and RADIUS, by interfacing with a unified account management and authentication system. Authentication and authorization are processed in real-time on a session basis, and by interfacing with standard protocols among various authentication systems—such as API, SAML, RADIUS, and TACACS+—it is possible to maximize both authentication efficiency and security. Network access management has evolved beyond traditional perimeter-based controls to operate an integrated framework of granular authentication, authorization, and monitoring. This advancement proactively addresses diverse threats both inside and outside the network and serves as a fundamental pillar in enhancing the overall security reliability of the organization.

5. Software-Defined Perimeter (SDP)

In a Zero Trust environment, Software Defined Perimeter (SDN/SDP) emerges as a pivotal technological domain that facilitates the virtualization of networks and the dynamic establishment of logical boundaries. This approach significantly diminishes the network attack surface and enables meticulous control over access to critical data and services. By redefining traditional physical boundary-based network security in a logical manner, Software Defined Networking (SDN) and Software Defined Perimeter (SDP) employ technologies such as policy-based routing, network segmentation, and dynamic access control to partition the network into multiple logical zones.

The establishment of logical boundaries based on SDN/SDP involves defining multiple logical zones within a network, grounded on the network and system architecture. The crux of this approach lies in differentiating access policies and authentication/authorization standards for each zone. By integrating distinct gateways and authentication systems for each logical boundary, the trustworthiness of identifiers, devices, and applications is meticulously verified through a multi-layered process before granting access. Furthermore, by interfacing with an integrated monitoring system, it becomes feasible to achieve real-time visibility of logically segregated network zones and to dynamically apply policies specific to each boundary.

In particular, within SDN/SDP environments, the verification of user identity serves as the foundational step for accessing any resource. Beyond the inherent authentication mechanisms of SDN/SDP, integration with account and identity management systems such as IAM and ICAM facilitates a multifaceted validation of the user's identity, behavior, and associated risk levels. During initial access, it is imperative to verify user ID and credentials, with the option to selectively implement various authentication methods, such as MFA and passwordless authentication, tailored to the specific environment. Furthermore, by employing pre-authentication technologies like Single Packet Authorization (SPA), it is possible to enhance the security of the entire user session through single-packet-based authentication that includes trusted information and continuous authentication verification. The software-defined perimeter based on SDN/SDP transcends the traditional boundaries of network perimeters, playing a pivotal role in elevating the security reliability of an organization's network by integrating real-time visibility, dynamic control, and granular authentication and authorization policies.

6. Network Segmentation

In a Zero Trust environment, network segmentation serves as a pivotal control mechanism to minimize the attack surface and effectively thwart the propagation of threats that may arise within the network. Traditional networks were structured in such a way that numerous systems and services could communicate freely across a single expansive topology. However, within a Zero Trust architecture, the network is logically divided into multiple zones, with each zone subjected to granular security policies and control standards to prevent lateral movement.

Macro Segmentation involves the division of a network into subnets, VLANs, or system groups to regulate traffic flow and delineate network zones based on high-level criteria such as function, department, or location. By distinctly separating inter-departmental segments or critical systems from general user areas, it facilitates the effective management of network traffic and prevents internal threats or attacks from proliferating across the entire network. Utilizing traditional network segmentation technologies such as firewalls and VLANs, it logically manages infrastructure and systems by group, enabling swift adaptation to changes through integration with real-time monitoring systems. In an automated environment, Macro Segmentation allows for the automatic implementation of additions, modifications, or divisions of network groups in accordance with established policies.

Micro-segmentation represents an advanced approach to network partitioning, surpassing macro-segmentation by operating at a more granular level. Unlike traditional boundaries such as subnets and VLANs, micro-segmentation meticulously delineates network assets and traffic based on diverse criteria, including applications, users, workloads, and data types. This method dynamically applies customized access policies and control standards at the level of individual groups or labels. By integrating with inventory, authentication, and asset management systems, it facilitates the implementation of specialized protective measures tailored to critical assets or zones. Micro-segmentation enhances the early detection of security threats within the network and supports automated policy adjustments or blockages in response to anomalous traffic or suspicious activities. When deployed enterprise-wide, it ensures that segmentation policies are updated in real-time, accommodating system and data changes, thereby enabling a flexible and responsive security posture.

In a zero-trust environment, network segmentation strategies transcend mere physical boundaries by integrating granular access controls and automated policy management tailored to the diverse operational environments and asset characteristics of an organization. This approach not only minimizes risks within the network but also simultaneously achieves effective prevention of internal threat propagation and the realization of a flexible security framework.

7. Network Flexibility

In a zero-trust environment, network flexibility constitutes a critical management and operational element to ensure business continuity and service availability, notwithstanding unpredictable disruptions, performance degradation, and a myriad of threats.

Network flexibility is constructed around three pivotal axes: availability, resilience, and backup management.

Firstly, ensuring network availability aims to guarantee the normal operation of the network not only under regular conditions but also in the event of disruptions. Organizations must establish a comprehensive management framework that includes network failure prevention, rapid detection and recovery from disruptions, real-time performance monitoring, preventive maintenance systems, and real-time alerts and reporting. Through these measures, the objective is to minimize network downtime and consistently maintain business and service continuity.

Network resilience refers to the capability to swiftly restore network components, configurations, and data through manual or automated procedures in the event of a disruption, thereby minimizing the duration of network service outages. Based on preparatory measures such as redundancy of critical segments and periodic failover testing, actual disruptions trigger automatic restoration in accordance with recovery policies integrated with the network backup systems. Ideally, in conjunction with next-generation network technologies like Software-Defined Networking (SDN) and Software-Defined Perimeter (SDP), the monitoring and response systems should autonomously diagnose anomalies and execute automatic recovery.

Finally, network backup management refers to a system that regularly backs up network components, configurations, and data either manually or automatically, thereby enabling swift restoration based on backup data even in emergencies such as failures or errors. Organizations must enhance the stability and availability of backup data by utilizing various types of backups and storage solutions. Additionally, they should implement security features such as encryption and compression to prevent the risk of backup data breaches or tampering.

Network flexibility serves as a structural foundation in a zero-trust environment, enabling the organization to address unforeseen and diverse risks while maintaining business continuity.

8. Network Monitoring and Analysis

In a zero-trust environment, network monitoring and analysis serve as a pivotal management framework that detects and analyzes the network's status, traffic flow, and anomalies in real-time, thereby facilitating the early detection and response to threats. As networks become increasingly complex and expansive, securing 'visibility' across the entire infrastructure becomes indispensable. The sophistication of the monitoring and analysis system significantly influences the capability to respond to security threats.

Securing network visibility entails the precise comprehension of the network's status, configuration, equipment changes, and topology through real-time monitoring. Organizations must establish visibility policies based on their network inventory and critical network segments, integrating asset management and monitoring systems to automatically ensure visibility whenever changes occur. This approach enables the comprehensive identification of real-time changes, connection statuses, and potential security threats within the network, segmented by equipment and zones.

Network monitoring involves the real-time examination of traffic flow, performance metrics, access logs, and anomalous traffic. It is imperative to establish an automated response system in conjunction with detection and response systems. In a zero-trust environment, it is essential to extend beyond traditional network monitoring, which primarily focuses on TCP/IP traffic, to include real-time monitoring and analysis frameworks for various traffic types such as DNS, ICMP, and SCTP. Regarding DNS traffic, inherent vulnerabilities such as spoofing, abnormal queries, and cache poisoning necessitate the real-time analysis of DNS traffic usage, patterns, and anomalies. Automated policies should be employed to modify DNS server settings or reset caches as needed. Similarly, other network traffic types, including ICMP and SCTP, require periodic and automated analysis to detect potential threats and diagnose network conditions.

Network traffic analysis is a comprehensive process that involves the collection, analysis, and visualization of all traffic within an organization. This process meticulously examines traffic patterns, anomalous behaviors, and potential indicators of cyber-attacks. By leveraging real-time analytical data, it integrates seamlessly with monitoring and detection systems, thereby facilitating automatic responses to security threats and optimizing network performance in a practical manner. Establishing a structure that enables the immediate detection, analysis, and response to anomalous traffic through the integration of various security systems is of paramount importance.

Ultimately, the enhancement of network monitoring and analysis systems elevates the transparency of the entire organizational network and bolsters real-time response capabilities, thereby providing a substantive foundation for the 'continuous verification' and 'automated response' demanded in a zero-trust environment. It is crucial to establish a structure that enables the immediate detection, analysis, and response to anomalous traffic by integrating with various security systems.

9. Network Resource Management

In a zero-trust environment, the lifecycle management of network resources entails the systematic administration of the entire lifespan of all network components, including switches, routers, firewalls, and virtual networks, from their introduction and operation to modification and decommissioning.

Organizations must integrate a variety of functionalities, including the provisioning (automated deployment) of network resources, real-time monitoring, policy-based automated response, reporting, and analysis. This integration enables them to comprehensively oversee and manage changes in the status of each resource, usage history, compliance with operational policies, and potential risk factors.

In particular, given the dynamic nature of network environments, which may lead to a myriad of events such as the deployment, reconfiguration, decommissioning, and disposal of equipment, it is imperative to manage all resources in a manner that ensures they possess a lifecycle defined by policy and telemetry-based parameters.

Through the integration with automated change management systems and monitoring tools, it is possible to manage the lifecycle of network environments and resources in real-time. Additionally, a framework must be established to enable swift automatic responses in the event of unforeseen failures or security threats.

In institutions with a high level of maturity, the automation and management of network resource creation, termination (initiation and expiration), and modification events are executed based on Infrastructure as Code (IaC). This approach enhances operational efficiency, stability, and security concurrently throughout the entire lifecycle of resources. The refinement of policies and processes is an indispensable foundation for maintaining a consistent security posture across devices and endpoints, as well as for facilitating swift risk response in an evolving work environment.

10. Network Policies and Processes

In a Zero Trust Architecture, network security policies and processes serve as the foundational cornerstone for consistently maintaining an organization's security posture and swiftly responding to evolving threats. It is imperative that network operations and system operations are conducted separately, ensuring that security policies are established based on the principle of least privilege, thereby allowing user access solely to necessary services. Every detailed process, including network operation and maintenance, change requests, equipment and configuration management, and remote equipment management, must encompass clear guidelines, designation of responsible parties, risk analysis and response strategies, and the management of policy change histories.

The network access policy is delineated from various perspectives, including unauthorized access control (such as IP management and device authentication), service and port blocking, and authentication processes. It must be sophisticatedly enhanced through real-time monitoring, anomaly access detection, and automated access restrictions, tailored to the level of importance and business objectives. Similarly, network architecture management necessitates periodic reviews and updates of the structure, alongside the automated management of topology maps and the integration status of equipment.

In the context of managing remote network equipment, the operation of information systems from outside the secure zone should be fundamentally restricted. However, in unavoidable circumstances, a comprehensive array of protective measures must be established and implemented. These measures include obtaining authorization from the responsible authority, designating specific access terminals, setting defined parameters and durations for access, employing enhanced authentication protocols, implementing segment encryption, and ensuring the security of access terminals through means such as antivirus software and patches.

In recent times, not only on-premises environments but also diverse multi-cloud and hybrid network environments are becoming the standard within organizations. Consequently, existing policies and processes must be expanded and redefined to integrate with cloud-native infrastructure. Additionally, it is imperative to consider the automation of policy implementation, the flexibility of policies in response to environmental changes, and the establishment of an integrated monitoring and audit framework.

Based on the aforementioned key elements, the device and endpoint pillar serves as the practical security control axis of a Zero Trust Architecture. By meticulously managing and verifying the reliability and security status of all devices within the organization in real-time, it ensures consistent control not only over the user's identity but also over the risks associated with the devices utilized for actual access. This approach effectively safeguards critical assets from both internal and external threats, while providing the flexibility and scalability necessary to swiftly respond to evolving work environments and advancing cyber threats. The enhancement of the device and endpoint pillar forms the foundation upon which an organization's security policies and management processes are substantively implemented.

Within a Zero Trust Architecture, the network pillar represents the most critical pathway that determines the overall security and reliability of data, systems, users, and devices, owing to the structural characteristics of organizations where all IT assets and services are interconnected through the network. It is also the focal point where security threats are most concentrated.

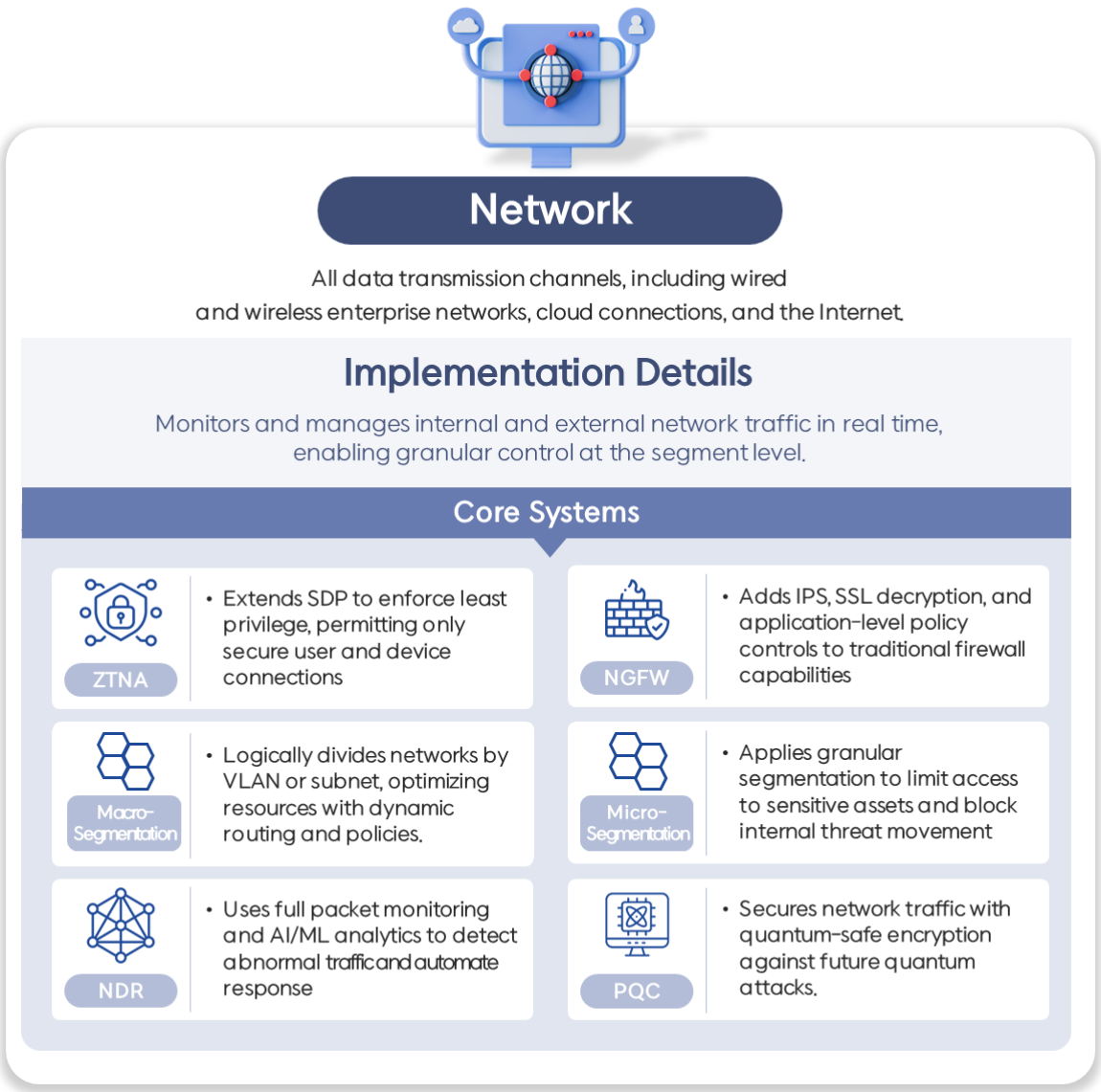
In particular, within a zero-trust environment, all traffic and connections are regarded as potential threats, irrespective of whether they originate from within or outside the network. It is imperative that diverse managerial and technical elements are seamlessly integrated, including real-time visibility acquisition, the application of dynamic and granular policies, traffic encryption, segmentation, access control, logical boundary establishment, and resilience assurance.

Through this, organizations can achieve early detection of threats across the entirety of network flows and realize a structure that enables automated control and response. The advancement of network pillars serves as a tangible foundation for the consistent application of zero-trust principles across the organization's entire infrastructure. It acts as a pivotal force in completing a digital security framework that can swiftly and flexibly respond to the rapidly changing IT environment and evolving security threats.

■ Implementation of Zero Trust Features for Key Systems

To successfully implement a Zero Trust environment, the deployment of technical solutions and systems capable of executing these solutions is indispensable. The Zero Trust architecture is founded on the principle of "never trust, always verify." To actualize this principle, it is essential to have systems in place that can assess the network status, continuously verify credentials, and ensure the enforcement of least privilege access.

The following key systems each play a pivotal role within a zero-trust environment, and these systems are interconnected to fortify the organization's security posture. This report aims to examine in detail the functions that must be performed by each system to implement a zero-trust environment and the resultant security enhancement effects that the organization can achieve through these implementations.



* Source: SK Shieldus, "The Inception of Zero Trust: Perfected with SKZT"

Figure 2. Key Network Systems

1. ZTNA (Zero Trust Network Access)

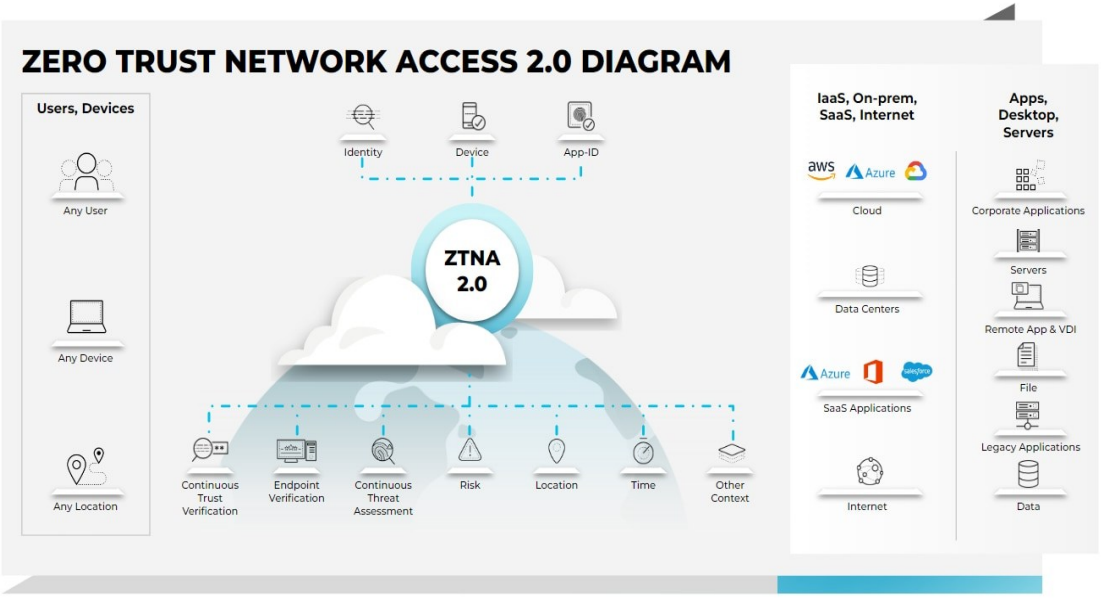
ZTNA, or Zero Trust Network Access, epitomizes a quintessential technology that applies the access control model, encapsulated by the core principle of Zero Trust Architecture: "never trust, always verify," to the network domain. This approach fundamentally diverges from traditional perimeter-based network access models, which are predicated on trust.

In a Zero Trust Network Access (ZTNA) environment, no network access request is inherently trusted. Instead, a comprehensive verification process is conducted in real-time, scrutinizing a multitude of contextual information such as user identity, device status, location, time, and behavioral patterns. Only after this rigorous validation is completed, access is granted exclusively to authorized traffic, allowing it to interact with internal networks and resources. This approach ensures the provision of a consistent access control framework that is uniformly applied to both internal (on-premises, in-office) and external (remote, cloud-based) environments.

Initially, Zero Trust Network Access (ZTNA) emerged based on Software-Defined Perimeter (SDP) frameworks. However, it has now evolved to integrate with a myriad of network access technologies, such as next-generation firewalls, Network Access Control (NAC), and VPN/SSL-VPN, with each vendor and solution offering its unique implementation. In the actual market landscape, ZTNA is distinguished not only as an "architectural concept" but also as discrete products or solutions provided by various vendors. There exists a substantial divergence in the functionalities supported and the detailed implementations, contingent upon the mode of adoption and the foundational origins of each solution.

For instance, the Next-Generation Firewall (NGFW)-based Zero Trust Network Access (ZTNA) meticulously regulates access by identifying user identities and device statuses, employing application awareness, and implementing granular policy-based access control and micro-segmentation. This ensures that only authorized users or devices can access specific network segments. In contrast, Network Access Control (NAC)-based ZTNA is predominantly optimized for internal network environments, such as corporate LANs. It operates by continuously assessing the status of endpoints, authentication credentials, and security inspection results, such as patches and antivirus updates, in real-time to permit or deny network access. Furthermore, VPN or SSL-VPN-based ZTNA has evolved by integrating additional verification elements—such as user and device authentication, Multi-Factor Authentication (MFA), and location and behavior analysis—into the traditional remote access framework. This evolution facilitates both granular access control and enhanced security in remote environments.

The ZTNA system is predominantly comprised of the Policy Decision Point (PDP) and the Policy Enforcement Point (PEP). The PDP meticulously evaluates a myriad of contextual information, such as user identity, device status, location, and behavioral patterns, each time a network access request is initiated. This comprehensive assessment dynamically determines the permissibility and scope of access. Subsequently, the PEP intermediates and regulates access to the actual network or resources exclusively for authorized requests. ZTNA is thus capable of being flexibly deployed across diverse environments, including on-premises, cloud, and hybrid settings. In recent developments, it has been integrated with cloud-based platforms like SASE (Secure Access Service Edge) to consistently implement zero trust access control in distributed infrastructure environments, such as remote work and multi-cloud scenarios.



* Source: Paloalto, “What is Zero Trust Network Access”

Figure 3. Palo Alto ZTNA 2.0 Diagram

ZTNA (Zero Trust Network Access) operates on the principle of treating all traffic, sessions, and connections as potential threats, irrespective of whether they originate from within or outside the network. This approach is pivotal in achieving real-time visibility, applying dynamic policies, and completely blocking unauthorized or vulnerable users and devices from access. Furthermore, it effectively prevents lateral movement through segmentation, thereby addressing the essential security demands of contemporary network environments. The implementation of such systems varies significantly based on each vendor's technological foundation—be it firewalls, Network Access Control (NAC), or Virtual Private Networks (VPNs)—and is influenced by factors such as optimization levels for different network environments (internal, external, cloud), policy granularity, authentication integration, user experience, and operational efficiency. Consequently, when considering the deployment of ZTNA, it is imperative to meticulously design and select solutions that are aligned with the organization's specific environment and operational characteristics.

2. NGFW (Next-Generation Firewall)

The Next-Generation Firewall (NGFW) represents a sophisticated evolution in firewall technology, integrating traditional firewall capabilities with advanced security features to address the multifaceted challenges of modern cybersecurity landscapes. Unlike conventional firewalls that primarily focus on packet filtering, NGFWs incorporate deep packet inspection, intrusion prevention systems (IPS), and application awareness to provide a comprehensive security solution. These firewalls are adept at identifying and controlling applications regardless of port, protocol, or evasive tactics employed by cyber threats. Furthermore, NGFWs offer enhanced visibility into network traffic, enabling organizations to enforce granular security policies and respond swiftly to emerging threats. By leveraging threat intelligence and machine learning algorithms, NGFWs can dynamically adapt to the ever-evolving threat environment, ensuring robust protection against sophisticated cyber attacks.

The Next-Generation Firewall (NGFW) represents an evolution beyond the traditional perimeter defenses that rely solely on IP and port-based mechanisms. It is a sophisticated network security system capable of identifying and meticulously controlling network traffic at the application level. The mere restriction of traffic at the network layers (L3, L4) is insufficient to accommodate the diverse application usage and security demands dictated by business objectives. NGFWs offer granular policies that permit applications aligned with business purposes, such as essential cloud services, Software as a Service (SaaS) like Microsoft 365 (M365), and specific social networking services (SNS), while selectively blocking unnecessary or high-risk services.

By integrating functionalities such as SD-WAN (Software-Defined Wide Area Network) and VPN/SSL-VPN, it is possible to achieve secure network connectivity and policy enforcement concurrently, even within distributed organizational environments such as headquarters, branch offices, and remote work settings. Logical network segments can be defined based on user, device, and application attributes, allowing for the implementation of distinct access policies for each segment. This approach effectively mitigates the spread of damage in the event of an internal breach. The architecture provides granular control over the flow of network traffic and enables the rapid isolation of specific areas upon the detection of anomalies or infections.

The Next-Generation Firewall (NGFW) functions as the central pillar of network security amidst the evolution of an organization's network environment into various forms such as on-premises, cloud, and SD-WAN. By enforcing policies based on diverse contexts, including applications, users, devices, and locations, it fundamentally enhances the overall security posture of the organization. Moreover, it serves as the technological foundation for the practical implementation of zero trust principles at the network level.

In recent times, traditional firewalls are gradually being phased out, with the integration of diverse security functionalities such as Intrusion Prevention Systems (IPS), DDoS mitigation, and application control becoming the standard in the form of Next-Generation Firewalls (NGFW) or Unified Threat Management (UTM) systems. These advanced configurations are increasingly being deployed and offered as the norm.

3. Macro-Segmentation

Macro-segmentation, within the realm of cybersecurity, refers to the strategic division of a network into distinct segments at a broad level. This approach is primarily designed to enhance security measures by isolating various sections of the network, thereby mitigating the risk of unauthorized access and potential breaches. By implementing macro-segmentation, organizations can effectively control and monitor the flow of data between these segments, ensuring that sensitive information remains protected against external threats. This segmentation strategy not only fortifies the network's defense mechanisms but also optimizes resource allocation and management, facilitating a more resilient and efficient cybersecurity infrastructure.

Macro-Segmentation represents a quintessential network segmentation technology designed to logically partition and control internal organizational networks. This advanced technique is predominantly implemented through sophisticated network equipment, such as next-generation switches based on Software-Defined Networking (SDN). Traditionally, networks were often delineated by a singular configuration or a limited number of boundaries. However, with the introduction of Macro-Segmentation, networks can be segmented into logical units such as VLANs (Virtual LANs) and subnets, allowing for precise control over traffic between each segment.

A notable advantage of SDN-based Macro-Segmentation lies in its capacity to define and automate network policies through software. Network administrators are empowered to logically segment the network based on application, user, and device attributes, independent of the physical location or hardware of network equipment. This capability allows for the application of policies to distinct segments. Consequently, it ensures the simultaneous enhancement of network agility, flexibility, and visibility, while enabling more granular control over network traffic flows and the enforcement of security policies.

Macro-segmentation represents an evolutionary advancement over traditional VLAN or physical boundary-centric network segmentation, primarily due to its capability to enforce policy control down to the application layer. By stringently restricting traffic flow between segments and preemptively blocking unauthorized access, it serves as the first line of defense in effectively obstructing the pathways through which threats propagate within an organization, such as lateral movement.

From the perspective of Zero Trust Architecture, Macro-Segmentation emerges as a pivotal technology capable of significantly enhancing the security posture of an organization's internal network. By subsequently extending into the more precise phase of Micro-Segmentation, a comprehensive internal security framework can be effectively realized. The logical boundaries and policy-based management established through Macro-Segmentation serve as a crucial foundation when expanded into Micro-Segmentation. This expansion facilitates more granular enforcement of security policies, enhances network visibility, and improves automated management efficiency, thereby augmenting the overall security capabilities of the organization.

4. Micro-Segmentation

Micro-segmentation, a sophisticated cybersecurity strategy, involves dividing a network into distinct, isolated segments at a granular level. This approach enhances security by enabling the implementation of stringent access controls and policies tailored to each segment, thereby minimizing the attack surface and preventing lateral movement of threats within the network. By employing micro-segmentation, organizations can achieve a higher degree of security customization and agility, allowing for rapid adaptation to evolving threats and compliance requirements. This method is particularly effective in environments with complex infrastructures, such as cloud computing and virtualized data centers, where traditional perimeter-based security measures are insufficient.

Micro-Segmentation represents a more granular security strategy compared to traditional Macro-Segmentation, meticulously partitioning the network at the OSI 7 layers (Application layer) down to the level of tasks, users, and applications. This sophisticated approach governs access by adhering to the principle of least privilege, thereby enhancing the overall security posture.

Traditional network segmentation has predominantly relied on physical and logical boundaries such as IP addresses, port-based configurations, and VLANs. In contrast, Micro-Segmentation focuses on logically dividing the network based on the relationships, purposes, and actual traffic flows between services and applications. This approach enables organizations to exercise precise control over potential threats or lateral movement by attackers within the internal network.

The implementation methods of Micro-Segmentation are broadly categorized into two distinct approaches.

The first approach is network-based Micro-Segmentation, which involves establishing logical boundaries at the application or user group level based on diverse contextual information such as user, device, location, access application, and traffic type, utilizing network equipment like NGFW (Next-Generation Firewall) and ZTNA (Zero Trust Network Access). This method enables real-time traffic analysis and allows for the immediate blocking of unauthorized access or anomalous behavior at the network layer.

The second approach involves system (host)-based Micro-Segmentation, wherein specialized solutions, either agent-based or agentless, are deployed at the endpoint level, encompassing servers and workstations. This method facilitates the implementation of granular security policies and access controls tailored to each individual terminal or server. During this process, the network connection structure (topology) is visualized, and the actual network traffic flow between various applications and services is meticulously analyzed to automatically generate and manage segmentation policies. Recently, the integration of AI and machine learning technologies has further enhanced this approach by autonomously optimizing network environments and policies, thereby augmenting operational efficiency through anomaly detection and policy recommendations.

Micro-segmentation, while conceptually aligning closely with the ideal objectives of network security, encounters various practical limitations in real-world applications, such as management complexity and the intricacy of policy design. Consequently, the latest solutions are evolving with a focus on advanced features like automation, visibility, and policy recommendation. These advancements are rapidly proliferating in actual implementation and operation scenarios across diverse sectors, including major domestic and international corporations and financial institutions.

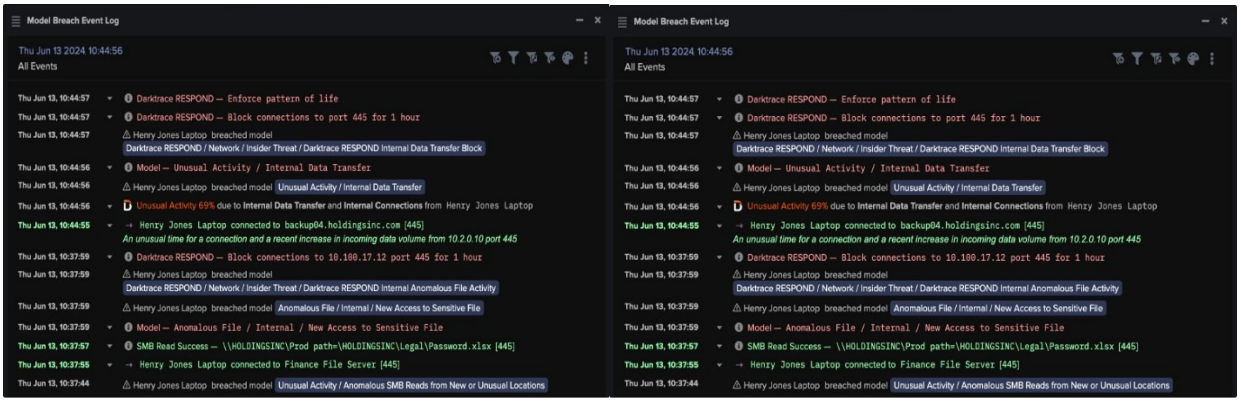
5. NDR (Network Detection and Response,)

Network Detection and Response (NDR) refers to a sophisticated cybersecurity solution designed to monitor network traffic for anomalous activities and potential threats. This system employs advanced analytics and machine learning algorithms to detect and respond to suspicious behaviors in real-time. By leveraging deep packet inspection and behavioral analysis, NDR provides a comprehensive view of network activities, enabling organizations to swiftly identify and mitigate cyber threats. The implementation of NDR is crucial for maintaining robust network security, as it enhances the ability to preemptively address vulnerabilities and ensures the integrity of sensitive data.

Network Detection and Response (NDR) is a pivotal network security system within a zero-trust environment, meticulously designed to detect and respond to a myriad of threats and anomalous activities. It achieves this by collecting and analyzing traffic across the entire network in real-time, utilizing full packet capture. This approach allows for precise threat detection and response, ensuring robust protection against sophisticated cyber threats.

One of the most salient features of Network Detection and Response (NDR) is its capability to store and analyze all traffic traversing both the internal and external network at the granularity of actual packet data, rather than merely detecting events at a simple log level. This functionality enables the real-time identification of a broad spectrum of threat scenarios, encompassing not only known attack signatures but also behavior-based anomaly patterns, abnormal communications, suspicious file transfers, and Command & Control (C&C) connections. The analyzed traffic data is instrumental in automatically generating a network topology map for the organization, thereby facilitating the visualization of the entire infrastructure's connectivity structure and traffic flow at a glance.

However, the implementation and operation of Network Detection and Response (NDR) in practical terms demand substantial resources and expertise. It necessitates an infrastructure capable of real-time storage and analysis of large volumes of traffic occurring across the entire network, along with complex rule sets and meticulously designed policies. Furthermore, it must be adaptable to diverse environmental changes, including on-premises, cloud, and IoT. Consequently, there may be significant personnel burdens and increased system complexity during the operational process. Nonetheless, with the recent expansion of machine learning and AI-based automation features, operational efficiency and detection accuracy have been significantly enhanced.



* Source: DarkTrace, "Utilizing Darktrace Antigena (AI) for Automated"

Figure 4. Analysis and Response to Network Intrusions Utilizing AI / Generation of Network Topology Map

6. PQC (Post-Quantum Cryptography, Quantum-Resistant Cryptography)

In the realm of cybersecurity, Post-Quantum Cryptography (PQC) represents a pivotal advancement designed to withstand the potential threats posed by quantum computing. As quantum computers continue to evolve, they threaten to undermine the security of conventional cryptographic systems, which rely heavily on the computational difficulty of problems such as integer factorization and discrete logarithms. PQC, therefore, emerges as an essential field of study, focusing on developing cryptographic algorithms that remain secure against the computational capabilities of quantum processors.

The significance of PQC lies in its proactive approach to safeguarding data integrity and confidentiality in a future where quantum computing could render current encryption methods obsolete. Researchers in this domain are tasked with the formidable challenge of devising algorithms that not only resist quantum attacks but also maintain efficiency and practicality for widespread implementation.

As the global community anticipates the advent of quantum computing, the urgency to transition to quantum-resistant cryptographic solutions becomes increasingly pronounced. This transition necessitates a comprehensive understanding of both quantum mechanics and advanced cryptographic techniques, underscoring the interdisciplinary nature of PQC research. Consequently, the development and standardization of PQC algorithms are critical to ensuring the continued protection of sensitive information in an era of unprecedented technological advancement.

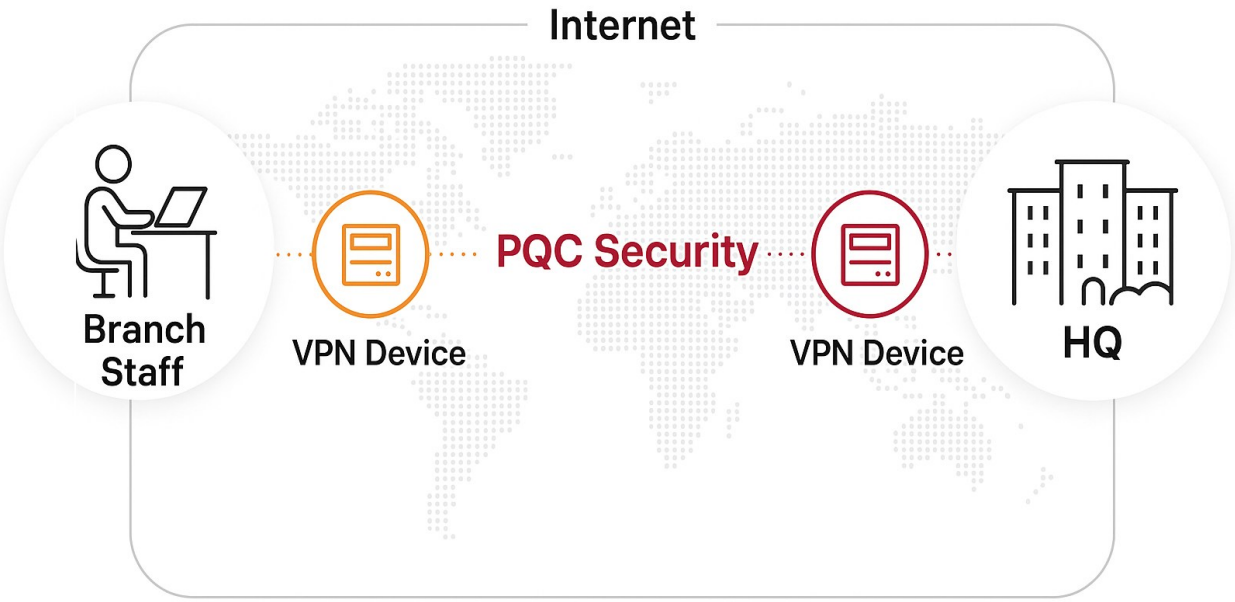
PQC, or Post-Quantum Cryptography, is an innovative encryption framework developed in response to the potential obsolescence of traditional public key cryptographic algorithms such as RSA and ECC, which may be rendered ineffective by the advent of fully operational quantum computers. Designed on the foundation of mathematical complexity that remains impervious to the computational prowess of quantum computers, PQC is increasingly recognized as a pivotal technology for the long-term safeguarding of networks and data.

Recently, the United States National Institute of Standards and Technology (NIST) has officially adopted three Post-Quantum Cryptography (PQC) algorithms as standards: ML-KEM, ML-DSA, and SLH-DSA. Encryption technologies based on these algorithms are progressively permeating various sectors of the industry.

The practical implementation of Post-Quantum Cryptography (PQC) solutions is manifested in various forms, including Quantum Encryption Communication Equipment (QENC/ROADM), Quantum Key Management Systems (QKMS), and Quantum Key Distribution (QKD). These solutions are being applied to a wide range of security-critical infrastructures, such as replacing traditional VPNs, encrypting communication channels, and issuing and managing certificates/keys. Gradually, they are being integrated alongside or as replacements for existing algorithms.

In a Zero Trust Architecture, encryption plays a pivotal role across the organization's security framework, encompassing networks, data, and authentication. The implementation of Post-Quantum Cryptography (PQC) is regarded as an essential strategy to proactively address future environmental changes. The adoption of PQC-based encryption is worth considering, given its resilience against threats that are challenging to defend against using traditional methods, such as external intrusions, man-in-the-middle attacks, and long-term storage attacks.

From a network perspective, Post-Quantum Cryptography (PQC) implements a key exchange and authentication framework that is secure against quantum computing threats, while providing the same user experience and policy framework as existing IPsec and SSL-VPN environments. This enables organizations to establish secure communication channels with a long-term, future-oriented outlook. Furthermore, it is feasible to either replace the existing infrastructure or integrate it in a hybrid manner by utilizing NIST-standard PQC algorithms, such as ML-KEM and ML-DSA.



* Source: SK Telecom, "SKT-SKB, First Commercialization of PQC (Post-Quantum Cryptography) on International Networks"

Figure 5. Conceptual Diagram of PQC-VPN

However, in the current practical landscape, there are not many instances where Post-Quantum Cryptography (PQC) has been commercialized and widely adopted. It is imperative to proactively review and engage in pilot applications in anticipation of the advent of quantum computing environments in the future.

The network pillar serves as the pivotal axis determining the practical implementation of a Zero Trust Architecture. Various network security systems, such as Zero Trust Network Access (ZTNA), Next-Generation Firewalls (NGFW), segmentation, Network Detection and Response (NDR), and Post-Quantum Cryptography (PQC), transcend their individual functionalities. They collectively undertake the responsibility of visually controlling the flow of all traffic within an organization and proactively detecting and mitigating potential threats.

In an increasingly diversified operational environment encompassing on-premises, cloud, headquarters, branch offices, and remote locations, it is imperative to meet a multitude of requirements such as granular traffic segmentation at the network level, real-time policy implementation, unified visibility, threat detection and response, and encryption. Throughout this process, each system must not serve a singular purpose but rather interoperate synergistically to consistently maintain the overall security posture of the network.

Through the organic integration of various systems within the network pillar, it is possible to reliably maintain network trustworthiness and security levels within a zero-trust environment.

■ Conclusion

The emergence of the Zero Trust architecture as a focal point can be attributed to the rapid transformation of work environments, transitioning from on-premises setups to cloud, hybrid, and remote work models, including telecommuting. This evolution has rendered organizational networks significantly more complex and has substantially broadened the attack surface. Consequently, within a Zero Trust environment, the network pillar adapts to these evolving conditions by effectively controlling connectivity across the entire organization. It functions as the central mechanism for verifying trustworthiness and responding to threats.

The network pillar has evolved beyond merely serving as a physical conduit for data transmission; it now constitutes a pivotal domain that comprehensively encompasses the connectivity framework and security controls of an entire organization. Given that every user's access, device connectivity, movement of operational data, and integration across cloud, branch, and headquarters are actualized through the network, the enforcement of policies and validation of trust within the network pillar become the definitive benchmarks that determine the overall security posture of the organization.

The essence of network fortification does not lie in the introduction of a singular system or the deployment of a specific solution. Rather, it necessitates the organic integration of a multitude of managerial and technical elements, such as network inventory, flow analysis, traffic encryption, access control, logical boundary configuration, segmentation, network availability, resilience, monitoring, and resource management. Only through such comprehensive integration can one simultaneously achieve substantial security performance and operational efficiency. Key systems like Zero Trust Network Access (ZTNA), Next-Generation Firewalls (NGFW), Network Detection and Response (NDR), and segmentation each play pivotal roles within their respective domains. However, they must ultimately be interoperable and integrated to consistently maintain the reliability of network flows, threat detection, and policy enforcement across the entire network spectrum.

The sophisticated technological configuration and operational strategy of network pillars lay the groundwork for implementing the fundamental principle of Zero Trust Architecture, "Never trust, always verify," within practical work environments. By enabling continuous verification of trustworthiness and real-time enforcement of security policies in complex network environments that range from on-premises to multi-cloud and from headquarters to remote workers, organizations can effectively mitigate security threats from both external and internal sources and enhance their security response capabilities.

In conclusion, the network pillar functions as the most fundamental and intrinsic axis of control within a zero-trust architecture. Strengthening the technical integration and unified management framework centered around the network pillar will serve as a practical and effective response strategy for organizational security in the future. By continuously advancing the sophistication of the network pillar and designing intricate policies, organizations will be able to maintain a robust security framework based on zero-trust, even amidst the complexly evolving digital environment and the escalating cyber threats.

■ References

[1] National Institute of Standards and Technology (NIST). 2020. “Zero Trust Architecture.” NIST Special Publication 800-207, August 2020.

[2] National Institute of Standards and Technology (NIST). 2022. “Guide to a Secure Enterprise Network Landscape.” NIST Special Publication 800-215, November 2022.

[3] U.S. Department of Defense (DoD). 2024. "Zero Trust Overlays." June 2024.

[4] National Cyber Security Center. 2025. "National Network Security System Security Guideline (Draft)." January 2025.

[5] SK Shieldus. 2025. “The Beginning of Zero Trust: Achieving with SKZT.” Brochure.

[6] Gartner. 2025. "Best Zero Trust Network Access Reviews 2025." Gartner Research, 2025.

[7] Gartner. 2025. "Best Network Detection and Response Reviews 2025." Gartner Research, 2025.

[8] IT Daily. 2025. “[ZTNA] 'ZTNA' Emerging as Next-Generation Network Security / Domestic and Global ZTNA Vendor Trends.” IT Daily, 2025.

[9] Darktrace. 2025. “The Most Advanced NDR Solution, Powered by Self-Learning AI.” Darktrace, 2025.

[10] Cato Networks. 2025. “Zero Trust Network Access (ZTNA).” Cato Networks, 2025.

[11] Palo Alto Networks. 2025. “What is Zero Trust Network Access.” Palo Alto Networks, 2025.

[12] Fortinet. 2025. “Zero Trust Network Access (ZTNA) to Control Application.” Fortinet, 2025

EQST INSIGHT

2025.07

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