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
06

SK shieldus

Contents

Headline

Rule Framework: A Core Tool for Threat-Centric Security Strategy

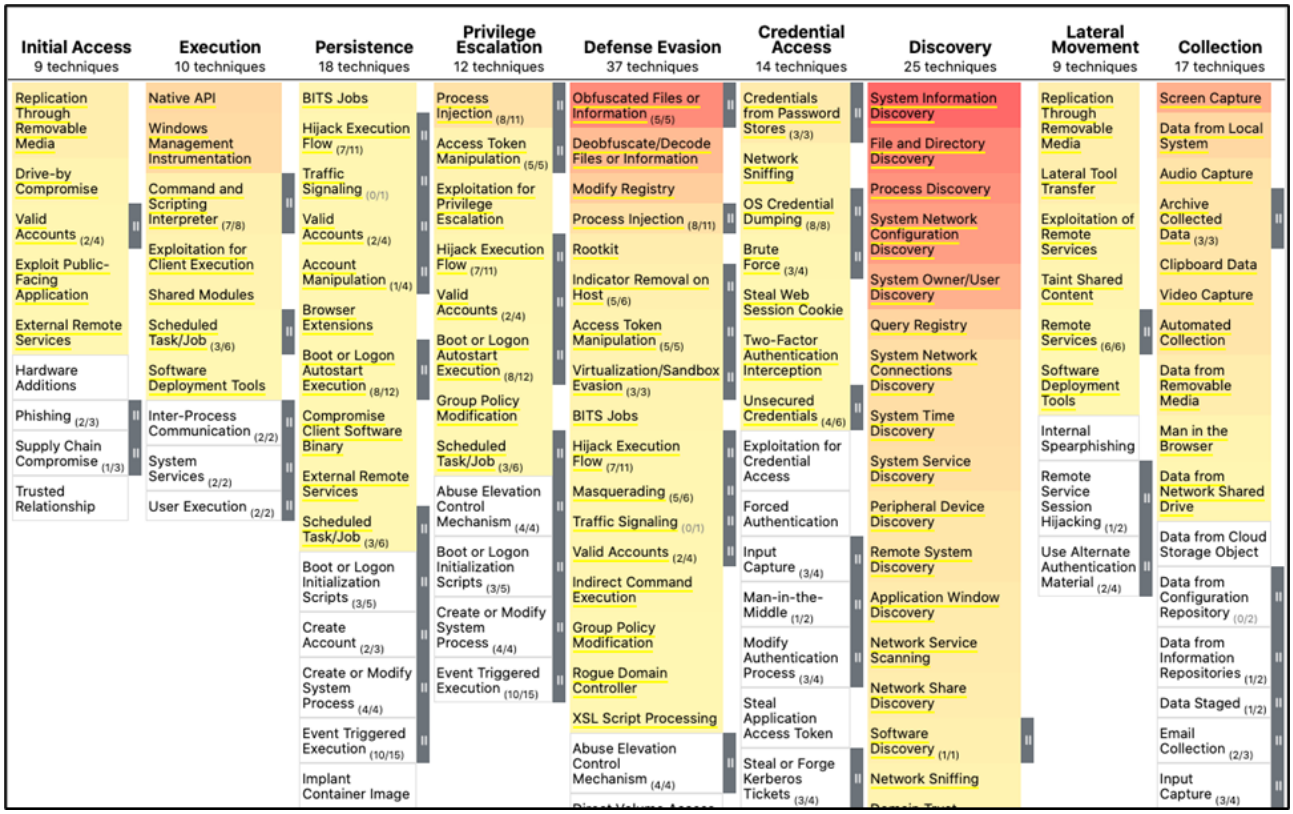
Ki-tack Seo / Security Operations & CERT Team, Team Leader

■ The Era of Advanced Persistent Threats

Cybersecurity is no longer just an IT issue; it has become a strategic priority directly tied to organizational survival. evolving into a strategic imperative intrinsically linked to the survival of organizations. Particularly, sophisticated attacks such as Advanced Persistent Threats (APTs), supply chain attacks, and ransomware are posing significant threats to major corporations and public institutions worldwide. Consequently, there has been a strategic shift in information security paradigms from traditional prevention-focused models to those centered on threat detection and response. At the core of this transformation lies the enhancement of detection rule-sets and methodologies, with the MITRE ATT&CK framework standing out as a quintessential security strategy model. The ATT&CK framework serves as a comprehensive knowledge base constructed on the actual behaviors of adversaries, thereby helping organizations design effective threat-focused security strategies.

■ What is the MITRE ATT&CK Framework?

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.



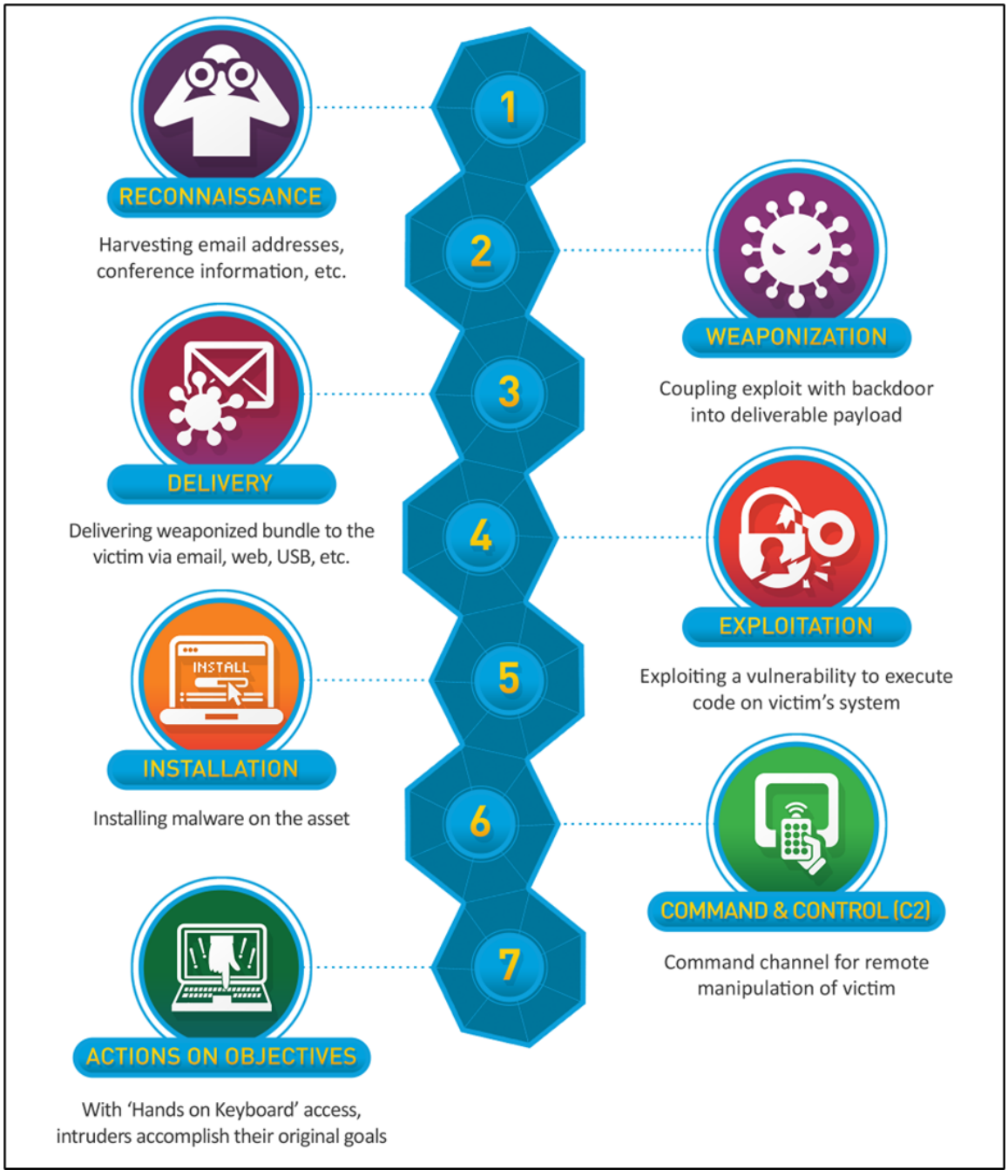
* Source: MITRE ATT&CK Official Website

Figure 1. Excerpt from the MITRE ATT&CK Matrix - Navigator

Attacks typically progress based on a series of sequential actions, with each phase distinguished by specific tactics and techniques. For instance, an attacker may initially attempt to gain initial access, followed by privilege escalation, internal reconnaissance, command and control (C2), and data exfiltration. The MITRE ATT&CK framework categorizes attacks according to these phases, offering detailed descriptions of techniques, detection indicators, and mitigation strategies. Currently, it provides three matrices: Enterprise, Mobile, and ICS, which can be applied to diverse environments such as corporate security, industrial control system security, and mobile security.

■ Composition of Tactics, Techniques, and Procedures (TTPs) in the MITRE ATT&CK Framework

The crux of the MITRE ATT&CK framework lies in its systematic modeling of adversarial behavior through distinct Tactics, which represent the stages of an attack, and the specific Techniques employed at each stage. This framework elucidates the objectives and methodologies utilized by attackers during the execution of a cyber assault, thereby enabling organizations to structurally analyze real-world threat scenarios.



* Source: Lockheed Martin Official Website

Figure 2. The Cyber Kill Chain Model Released by Lockheed Martin

As illustrated in [Figure 2], cyber threat activities unfold in a sequential manner. Delving deeper into each phase, the initial stage involves the attacker attempting 'Initial Access' to the system. This is executed through methods such as phishing emails, malicious links, or exploiting vulnerabilities in user behavior or external interfaces, including known user credentials. The primary objective of this phase is to establish a foothold that facilitates entry into the internal network. Subsequently, the 'Execution' phase ensues, wherein the attacker, having gained access, endeavors to execute malicious code to secure control over the system. This encompasses activities such as script execution, command injection, and the exploitation of processes. This phase serves as the gateway through which the attacker effectuates malicious operations within the system.

The term 'Persistence' refers to the mechanisms established by an attacker to maintain a prolonged presence within a system. Techniques such as service registration or the installation of autorun programs are employed to ensure that the malicious code continues to operate even after a system reboot or user logout. The subsequent phase, known as 'Privilege Escalation,' involves elevating the privileges of a standard user to those of an administrator or root, thereby enabling broader access to the system. Following this, the 'Defense Evasion' stage employs techniques to bypass or neutralize security solutions and logging systems. This includes methods such as obfuscating malicious files or employing code injection to circumvent antivirus software. This stage is critical for avoiding detection and facilitating ongoing attacks. During the 'Credential Access' phase, the attacker seeks to collect user IDs or passwords within the system to move laterally to other systems or to gain additional privileges. This is achieved by extracting password hashes from memory or installing keyloggers. The 'Discovery' phase involves the reconnaissance of the internal network's structure, user directories, and system information. Attackers utilize this intelligence to plan subsequent attack phases or to establish pathways for lateral movement.

The phase at which malicious activities begin to proliferate extensively is referred to as the 'Lateral Movement' stage. This involves the attacker transitioning from one system to another, employing methods such as credential theft or remote command execution as primary means. Through this process, the attacker gradually gains access to critical systems. Once the objectives of the attack become more defined, the 'Collection' phase commences. During this stage, the attacker accumulates specific data, such as documents, customer information, certificates, and log files, which are stored for potential future exfiltration or manipulation. The process of transmitting the collected information to external entities constitutes the 'Command and Control (C2)' phase. Here, the attacker establishes a connection with an external C2 server via malicious software, facilitating the exchange of commands or the transmission of data. Typically, encrypted communications or transmissions masquerading as legitimate protocols are employed.

The final phase of an attack is termed 'Impact,' which encompasses the actual infliction of damage, such as the degradation of system availability, data corruption, and ransomware infection. At this juncture, the attacker endeavors to achieve objectives such as data deletion, system destruction, and monetary extortion.

In this manner, the Tactics, Techniques, and Procedures (TTPs) of the MITRE ATT&CK framework clearly describe each phase of an attack, thereby facilitating the tracking and analysis of adversaries' mindsets and behavioral patterns. This enables threat response organizations to develop stage-specific defensive strategies and to construct more sophisticated detection rules and response scenarios.

■ Analysis of APT Attack Cases

Through real-world attack scenarios, one can comprehend the application of strategies and techniques from the ATT&CK framework in practical settings.

- APT29 (Cozy Bear)

In the SolarWinds supply chain attack, techniques such as DLL Side-Loading (T1574.002) and the injection of malicious code into legitimate processes (T1055) were employed.

- Lazarus Group

In attacks targeting financial institutions, a tactical combination of techniques was employed, including phishing (T1566.001), credential dumping (T1003), and lateral movement via SMB (T1021.002).

- FIN7

Malicious documents were distributed targeting POS systems (T1203), followed by data collection from local systems (T1005) and exfiltration of the gathered information to external servers (T1041).

In the aforementioned case, each attack flow is meticulously mapped to the MITRE ATT&CK techniques and tactics, thereby enabling the reconstruction of attacks or the formulation of detection policies. This approach transcends the mere enumeration of techniques employed by adversary groups, instead mapping their entire attack flow into a 'Tactics, Techniques, and Procedures (TTPs) framework.' This allows for the visualization of potential detection and response measures at each stage.

● Lazarus Group: Attacks targeting financial institutions and cryptocurrency exchanges. Lazarus Group, a threat actor reportedly linked to North Korea, is an APT organization that has consistently targeted financial institutions and cryptocurrency exchanges. Their operations typically involve gaining initial access through phishing emails, social engineering tactics, and exploitation of web vulnerabilities. Following initial compromise, they proceed to obtain credential access and conduct lateral movement within the network to reach high-value asset systems. When analyzed through the MITRE ATT&CK framework, Lazarus's phishing campaigns align with the T1566.001 technique (Spear Phishing Attachment). Subsequent privilege escalation is categorized under T1068 (Exploitation for Privilege Escalation), while credential theft corresponds to T1003 (Credential Dumping). The group also accessed internal systems via RDP connections (T1021.001) and exfiltrated sensitive data to external C2 servers (T1041). In practical cybersecurity operations, such correlation analysis enables security teams to incorporate the tactics and techniques used by Lazarus into detection policies. Moreover, it serves as a foundational reference for conducting effective threat hunting.

Table 1. Example of Applying the MITRE ATT&CK Framework to Analyze Attack Cases

As exemplified in APT cases, the MITRE ATT&CK framework facilitates a comprehensive understanding of complex attack vectors by tactically structuring the flow of these incursions. This enables a clear identification of the attack's origin, the techniques employed, and the stages at which detection and defense were feasible. Furthermore, it serves as an effective tool for constructing preemptive detection rules based on historical attack instances or for developing threat hunting scenarios.

■ Secudium Center – Rule Framework

The Rule Framework transcends being merely a theoretical tool, playing a pivotal role in enabling real-world security organizations to systematically comprehend adversarial behaviors and enhance their response capabilities. At the Secudium Center, which oversees SK Shieldus's remote monitoring services, a proprietary Rule Framework utilizing the MITRE ATT&CK framework has been integrated into the monitoring platform "Secudium v2.0." The implemented framework is structured into nine stages within major categories, adopting a detection strategy that classifies collected information into essential and optional data. This approach allows for the organic application of threat identification and response.

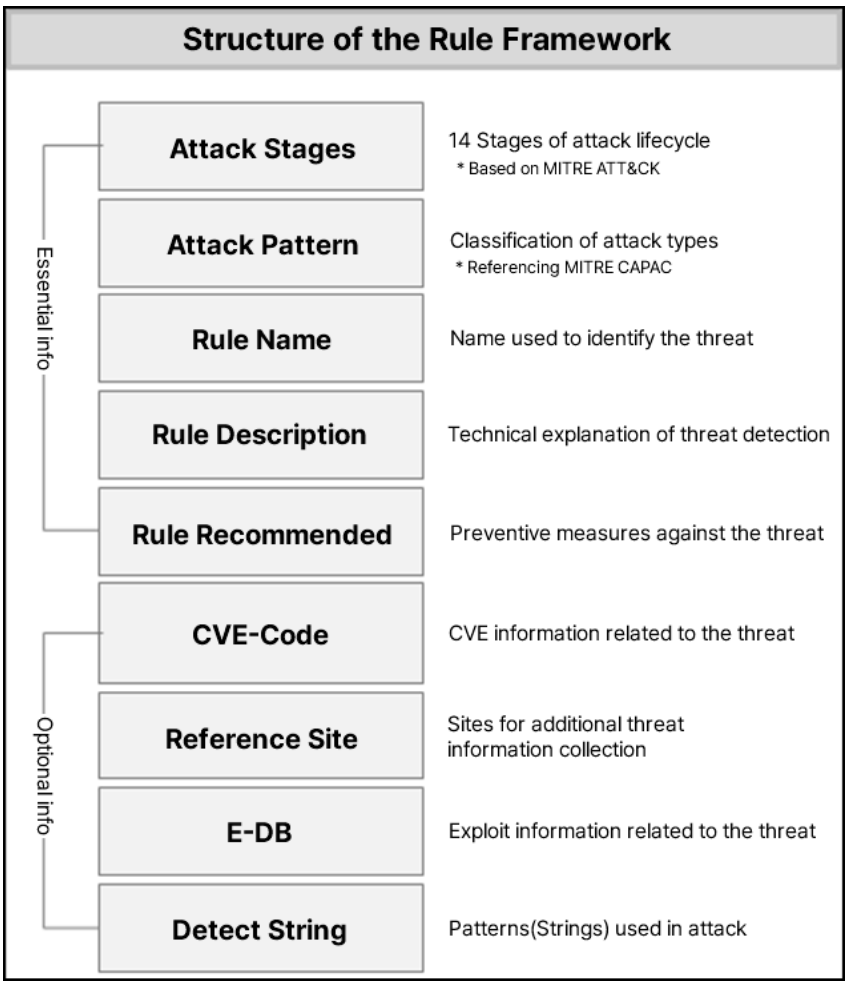


Figure 3. Structure of the Rule Framework Applied to the Secudium Monitoring Platform

The core objective of utilizing the specified Rule Framework lies in detecting and classifying threat logs collected through this system, thereby establishing a threat response mechanism that incorporates appropriate countermeasure technologies. Furthermore, by selecting specific features of Threat Hunting, it becomes possible to proactively detect techniques employed by attackers, thereby preventing the proliferation of damage and enhancing the potential for response at the initial stages of an attack.

The key to success in information security against sophisticated cyber attacks lies in 'systematic integration and iterative improvement.' From this perspective, defining a detection methodology utilizing a Rule Framework is not merely about adding new tools; rather, it is a process of redesigning the entire security operation into a threat-centric response system. By systematically classifying and operating strategies and technologies while concurrently exploring potential recurring threats, it becomes possible to establish a "proactive security system" that stays one step ahead of the attackers.

References

[1] MITRE ATT&CK: https://attack.mitre.org

[2] Red Canary: https://redcanary.com

[3] Mandiant Threat Intelligence Reports

[4] Atomic Red Team: https://github.com/redcanaryco/atomic-red-team

[5] Lockheed Martin – cyber kill chain: https://www.lockheedmartin.com

Keep up with Ransomware

Devman: A Single Group Using Assorted Ransomware

■ Overview

In May 2025, the number of ransomware incidents recorded was 484, reflecting an approximate 12% decrease compared to April's 550 cases. Although there has been a consistent downward trend in the number of incidents since March, the disclosure of the Vanhelsing ransomware source code in May has heightened the likelihood of the emergence of variants or groups exploiting this code.

In early May, the dedicated Leak Sites of LockBit was defaced with the phrase "Don't do crime CRIME IS BAD xoxo from Prague." Not only was the dedicated Leak Sites altered, but the administrative panel was also compromised, leading to the exfiltration of certain internal database files. The leaked database contained cryptocurrency wallet addresses, configuration information used by different versions of the ransomware, affiliate account details, and chat logs; however, it did not include the private keys used for decryption. This hacking incident has not only tarnished LockBit's reputation but also appears to have significantly disrupted its operations, as evidenced by the fact that the dedicated Leak Sites remained inaccessible until early June.

The source code of the Vanhelsing ransomware has been disclosed on the Russian hacking forum RAMP. A former member, known as th30c0der, uploaded a post on a related forum site indicating the sale of the Vanhelsing ransomware's source code. The Vanhelsing administrators acknowledged this and released portions of their existing ransomware and panel page source code. However, th30c0der introduced himself as the pivotal figure responsible for developing the panel, payment system, and the ransomware itself, asserting that the disclosed code does not represent the entirety of the source. He claims that the source code he is selling is the most recent version.

Meanwhile, a file presumed to be a decryption tool for Qilin ransomware has been discovered. This particular sample offers the capability to decrypt encrypted files using either the AES algorithm or the ChaCha20 algorithm. However, it has been confirmed that the decryption is not universally applicable to all Qilin ransomware variants; it functions correctly only when the files have been encrypted with specific versions or particular encryption keys.

In May, several incidents of breaches were identified domestically. The group initially operating under the name RaLord, which rebranded as Nova in May, claimed responsibility for attacking a domestic university, asserting that they exfiltrated internal documents, reports, portal site source codes, databases, and student information. In June, the exfiltrated data was disclosed; however, it did not include personal information, with only the portal site source code and database-related information being verified.

The TCR Team launched cyberattacks against two companies within the domestic finance and manufacturing sectors. These companies were categorized as having failed negotiations on a dedicated Leak Sites, leading to the partial exposure of their data. The compromised information was confirmed to include internal documents and employees' personal data. However, the data that had been disclosed was removed approximately two weeks later, and by the end of May, the dedicated Leak Sites had been deactivated, rendering it inaccessible.

A ransomware group exploiting a file upload vulnerability (CVE-2025-31324) in SAP's application integration and execution platform, NetWeaver, has been identified. Although this vulnerability was patched on April 24th, evidence has emerged indicating that the BianLian group and the RansomEXX group have exploited it. While neither group has deployed ransomware, activities have been detected involving the exploitation of the vulnerability to communicate with BianLian's command and control (C2)[1] servers or to distribute PipeMagic, a backdoor[2] commonly utilized by RansomEXX.

[1] C2 (Command and Control): A server that delivers commands to infected PCs or servers to perform attacker-specified actions.

[2] Backdoor: Malware that bypasses security mechanisms to grant access to the target system.

■ Ransomware News

Leak of Internal Database from LockBit Group

- Leaked intelligence indicates that the hacking incident transpired in late April while the exfiltrated data was made public in early May.
- A partial extract of the internal database was leaked, alongside a sarcastic remark "Don't do crime. CRIME IS BAD. xoxo from Prague."
- Attribution suggests that the operation was conducted by the same entity involved in the Everest group hack.

The decryption tool for the Qilin ransomware has been discovered.

- Qilin ransomware-encrypted files can be decrypted using the corresponding algorithm—either AES or ChaCha20—based on which was employed during encryption.
- The decryptor does not support all variants of the Qilin ransomware and operates successfully only when certain versions or matching keys are present.

Vanhelsing ransomware's source code has been publicly released.

- A user operating under the alias "th30c0der" attempted to sell the source code on the RAMP forum in May.
- The Vanhelsing operators acknowledged that the user had indeed collaborated with them and subsequently released their own ransomware source code.
- "th30c0der" claimed that the publicly released code corresponds to version 1, while asserting that he is selling the latest version, v2.

The TCR Team group carried out attacks against two South Korean companies.

- The group targeted finance and manufacturing companies, stealing and leaking sensitive data.
- The leaked data included internal documents and employee personal information.
- The DLS became inactive in late May and is no longer accessible.

The Nova group carried out an attack against a South Korean university.

- The group stated that it had infiltrated a South Korean university and extracted internal documents, source code, and student records.
- Although the data was published in early June, it did not include any personal information instead, it contained the source code and database of a portal site.

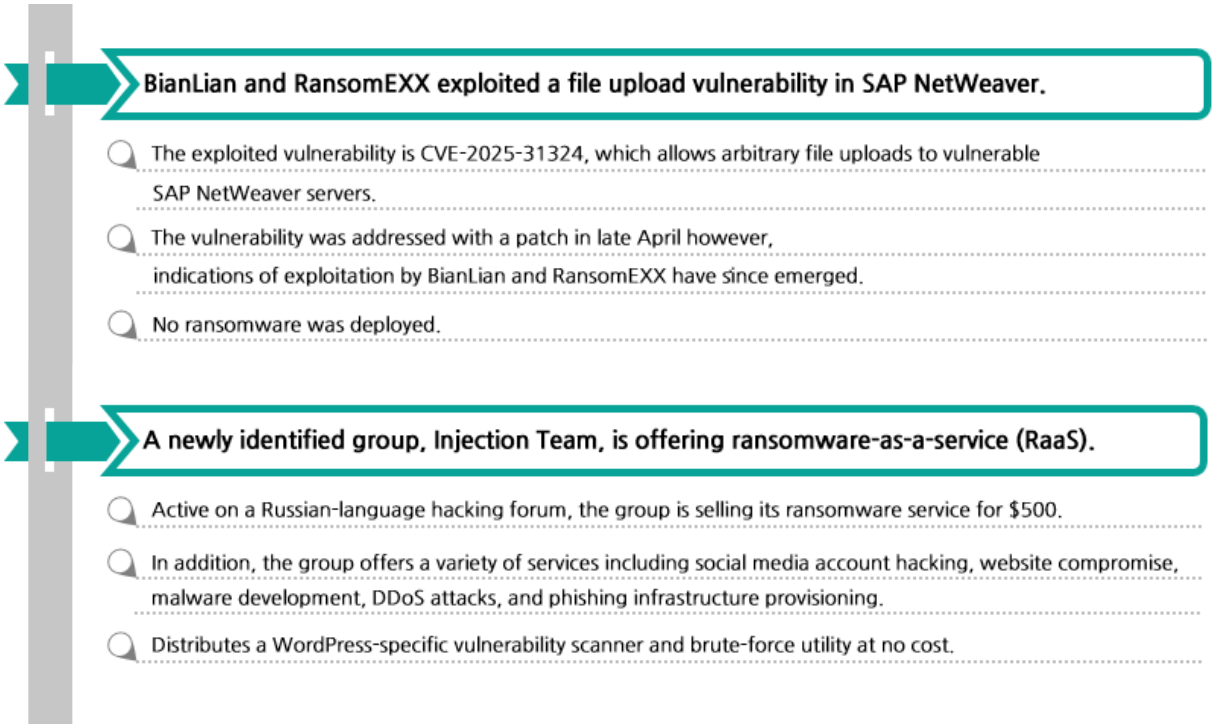


Figure 1. Ransomware Trends

Ransomware Threats

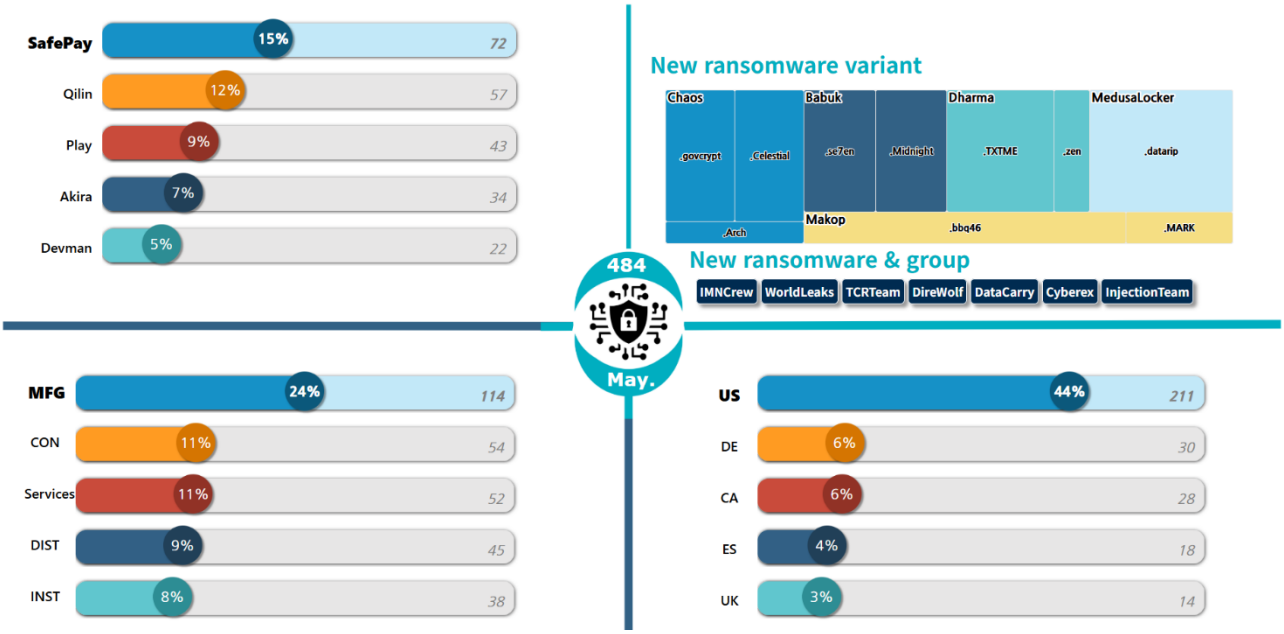


Figure 2. Status of Ransomware Threats in May 2025

New Threats

In May, a total of eight new ransomware groups were identified. It has been observed that JGroup uploaded 18 new victims, Imncrew 8, WorldLeaks 14, Direwolf 11, and DataCarry 10, each to their respective dedicated Leak Sites. Additionally, the Cyberex group does not operate a separate leak site; instead, it conducts ransom negotiations with infected victims solely through a chat site.

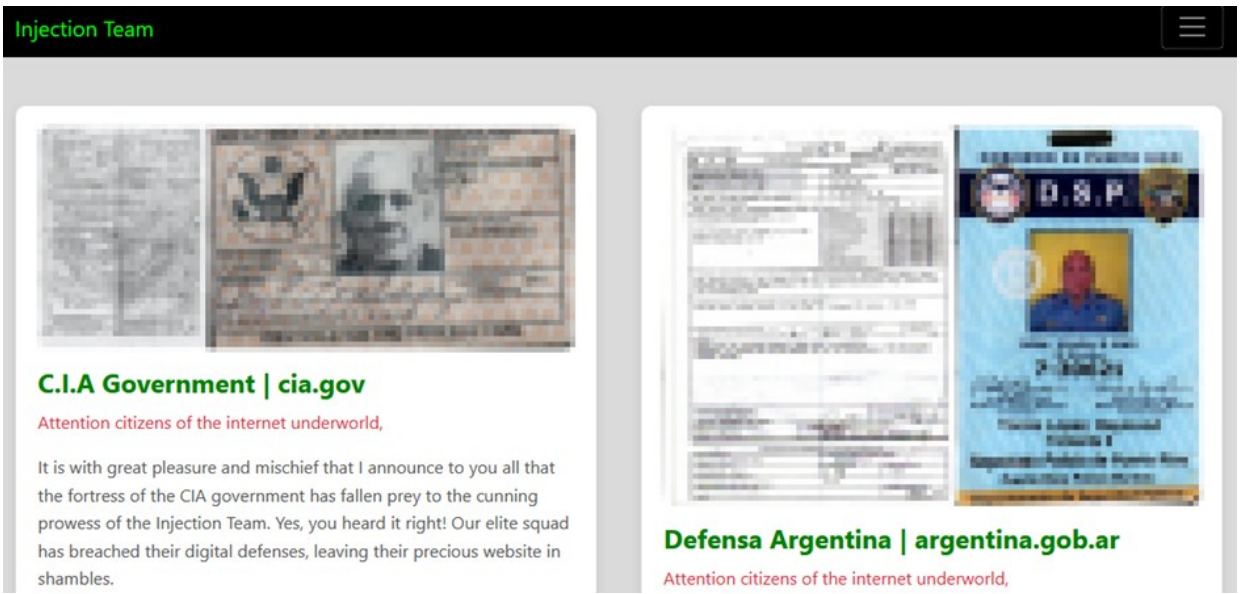


Figure 3. Injection Team Dedicated Leak Sites

The newly emerged group, known as the Injection Team, is actively promoting itself on Russian hacking forums. This group offers a wide array of services, including ransomware-as-a-service, social media hacking, website hacking, malware development, DDoS attacks, and phishing infrastructure provision, typically priced around $1,000. In addition to these paid services, they also distribute a vulnerability scanner for WordPress environments and brute force tools free of charge.

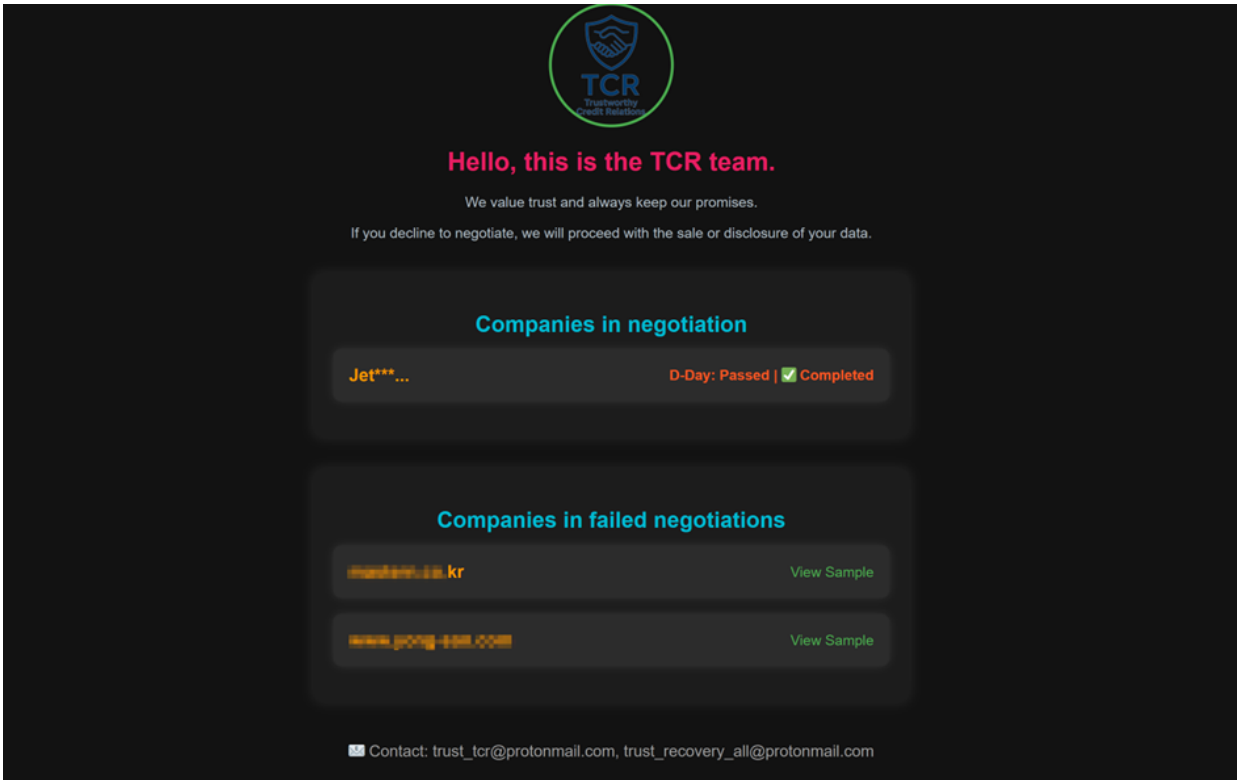


Figure 4. TCR Team Dedicated Leak Sites

A new group targeting domestic entities has also been identified. The attacks by the TCR Team group were discovered in May, during which they targeted two domestic companies and disclosed some of their data. The affected companies were identified as a financial investment firm and an automotive parts manufacturer, with compromised documents including internal corporate files and employee personal information. By the end of May, access to sample data became unavailable, and subsequently, the dedicated Leak Sites itself was deactivated.

Top 5 Ransomware

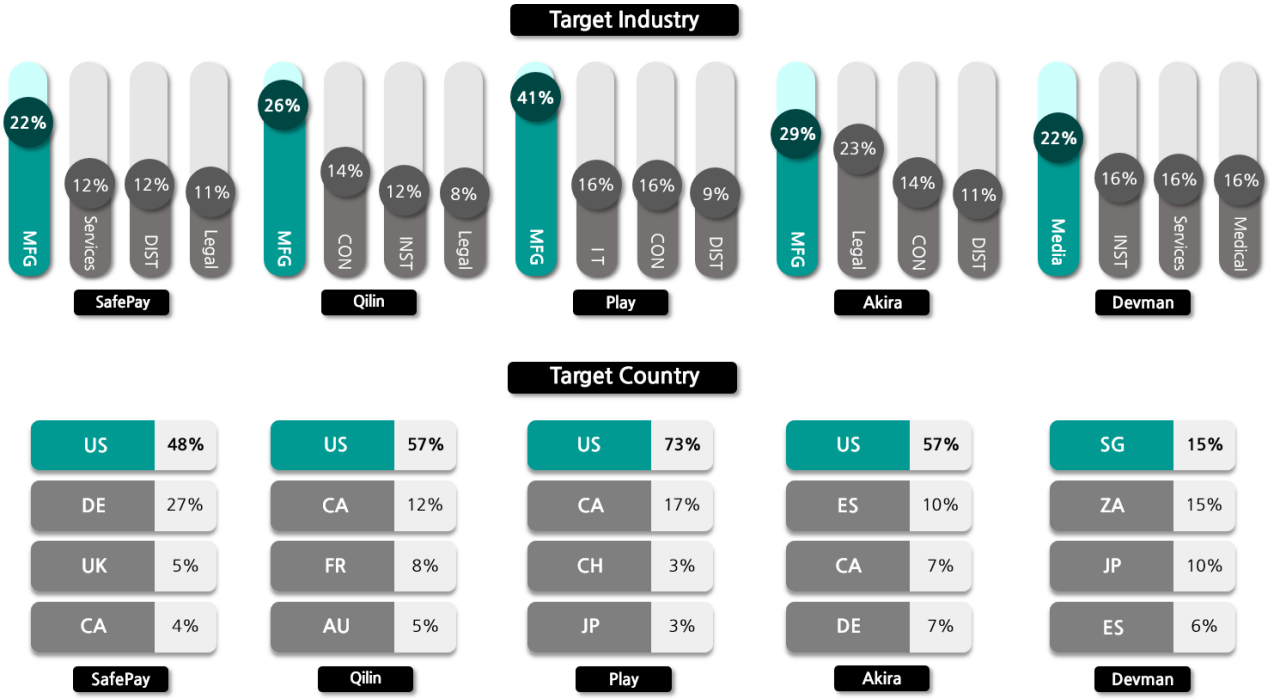


Figure 5. Overview of Major Ransomware Attacks by Industry/Country

The SafePay group launched an attack on the public high school Gymnázium a Jazyková škola Zlín, located in the Czech Republic, resulting in the exposure of approximately 30GB of internal data. This data encompassed not only internal school records but also included certain student information. Furthermore, the group targeted the Australian law firm RTB Legal, exfiltrating around 200GB of data. This breach led to the unauthorized release of a wide array of legal and administrative documents, including court documents, client information, emails, contracts, and wills.

The Qilin group launched an attack on the government of Cobb County, Georgia, USA, exfiltrating approximately 150GB of data comprising 400,000 documents. The compromised data included personal information of residents and government officials, as well as images of deceased individuals. Additionally, they targeted the Army Navy Country Club, a prestigious country club in the United States, and exfiltrated 300GB of data. This breach resulted in the exposure of sensitive information such as members' names, addresses, credit card details, and credentials.

The Play group has been exhibiting a pattern of targeting American enterprises with its cyber attacks. In May, it launched an assault on the U.S. construction firm W.E. Bowers, resulting in the exfiltration of a diverse array of data, including customer documents, budgets, payroll statements, accounting records, identification credentials, and financial information. The specific extent of the damage, however, has not been disclosed. Another U.S. construction company, Greater Seattle Concrete, also fell victim to an attack, leading to the exposure of internal documents and data containing confidential information at the end of May.

The Akira Group orchestrated a cyberattack on the American energy company Pacific Summit Energy, resulting in the exfiltration of approximately 160GB of data. This compromised data encompasses employee personal information, financial audit documents, and internal operational files, all of which have been fully disclosed. Furthermore, the group targeted the U.S. financial institution Flagship Bank, seizing and releasing 40GB of data that includes customer information, detailed financial records, and contractual agreements.

In April, a newly emerged group known as Devman claimed responsibility for an attack on Kenya's National Social Security Fund (NSSF Kenya), asserting that they exfiltrated approximately 2.5 terabytes of data. The group has been consistently uploading verification screenshots via their X (formerly Twitter) account, while also detailing their reconnaissance, data exfiltration, and file encryption methodologies on a dedicated Leak Sites. The compromised data reportedly includes personal information such as names, addresses, and social security numbers, with a ransom demand set at $4.5 million USD (approximately 6.1 billion KRW).

Additionally, the Philippine media outlet GMA Network reported that their internal servers were encrypted, resulting in the exfiltration of approximately 65 gigabytes of data. The ransom demand in this instance was $2.5 million USD (approximately 3.4 billion KRW). However, GMA Network asserted that the leaked data did not contain any sensitive or personal information.

■ Focus on Ransomware

Welcome to Devman's Place

Soon there will be some news. Thanks for waiting.

WE ARE ACTIVELY BUYING ACCESS TO COUNTRIES(UK, FRANCE, CANADA). THESE COUNTRIES ARE OUR MAIN PRIORITY.

P.S sorry for being offline

My Victims

Company	Status	Ransom Amount
Doumen.fr(QILIN)	Negotiating	800k USD
Optimax Technology(QILIN)	Whaitng	590k USD
Texas Construction Firm(QILIN)	Pending	Amount TBD
Tawasol (APOS Attack)	Pedning	150k USD
Feel Four (QILIN Attack)	Pedning	60k USD
China Harbour (s) Engeneiring Company (Dragon Force Attack) FILE SAMPLE 1 avaliable /CHEC/CHECsample.zip	Ecnrypted(we encrypted every signle device on the network and downloaded 50gb of sensitive files)	450k USD
Honk Kong Victim (To be discoled)	(To be discoled)	(To be discoled)

Figure 6. Devman Dedicated Leak Sites

The Devman group, which commenced its operations in April 2025, has thus far disclosed a total of 44 victims. Upon its initial emergence, the group exhibited a distinctive approach by meticulously detailing the software vulnerabilities or weak passwords exploited during attacks on its "My Writeups" page, delineating each phase of the attack process. Notably, instead of deploying proprietary ransomware, Devman has strategically leveraged ransomware from other groups, resulting in victims being listed not only on Devman's leak site but also on the leak sites of other ransomware collectives. The ransomware from other groups utilized in their attacks includes Apos, Qilin, DragonForce, and RansomHub. However, starting in May, they began to publish victims affected by their proprietary ransomware, known as Devman ransomware.

The Devman Group primarily operates on X (formerly Twitter), utilizing the platform predominantly for self-promotion. This includes showcasing pages for ransomware services under development, announcing impending attacks, and sharing videos demonstrating their custom-made ransomware. Furthermore, in cases involving companies with significant data breaches, the group has been observed to directly mention the victim's X account, releasing sample images of the data obtained or screenshots of the infiltrated environment as a means of mockery and intimidation.

TBD GREECE	ALL FILES ENCRYPTED 120gb of data stollen	NEGOTIATION STARTED
TBD HONK KONG	ALL FILES ENCRYPTED	PAYED
TBD KOREA	ALL FILES ENCRYPTED	PAYED

Figure 7. Victim List with Partial Information Disclosure

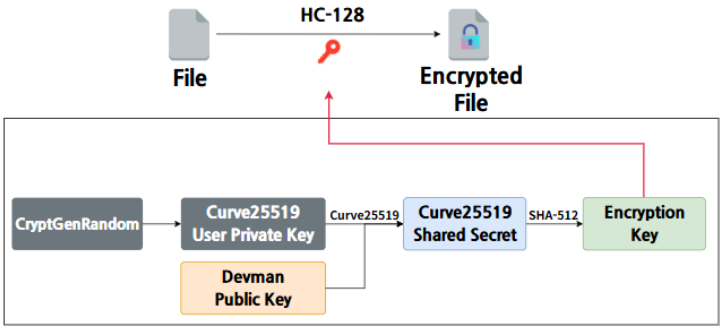
When disclosing victims, these entities do not immediately reveal the company name; instead, they first disclose the country to which the company belongs or the industry sector it operates within. Among these are domestic companies; however, the precise scale of the damage or the ransom demanded has not been disclosed, although it has been confirmed that the payment has already been made.

In May, a sample suspected to be the proprietary ransomware of the Devman Group was discovered, with the group acknowledging through their X account that this ransomware is indeed version 1. However, upon comparative analysis, it was found to be a version with additional functionalities, closely resembling the Mamona ransomware that was hacked last March. Starting in June, the group is expected to intensify its activities by launching its own ransomware service. In anticipation of this, we aim to share the analysis of the Devman ransomware to better prepare for potential threats.

Devman Ransomware

Encryption Key

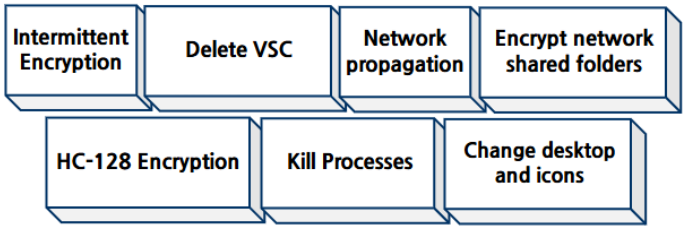
Generate encryption key using Curve25519 algorithm and encrypt files with HC-128



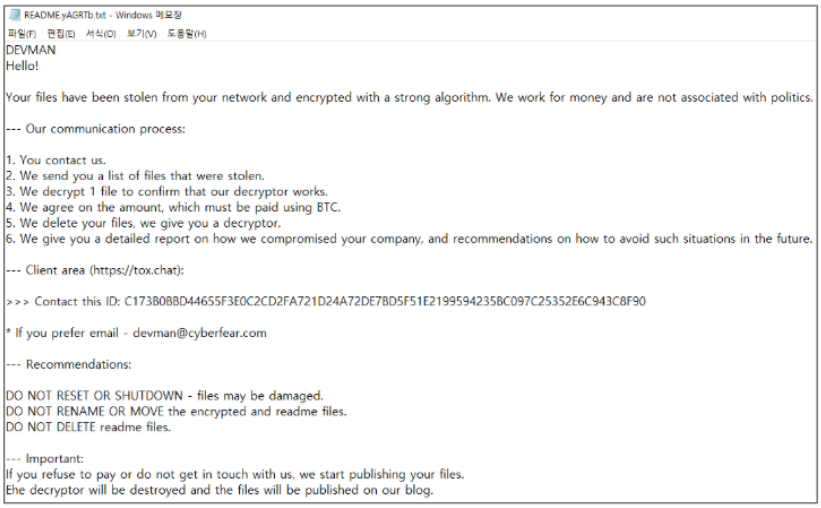
Encryption Method

* Encryptino Method 1.
  - Files ≤ 1MB: Encrypt entire file
  - Files > 1MB and ≤ 5MB: Encrypt the first 1MB of the file
  - Files > 5MB: Encrypt from the beginning of the file up to N% of the file size (max: 70MB)
* Encryption Method 2.
  - Files ≤ 64Bytes: Encrypt entire file
  - Files > 64Bytes and ≤ 5MB: Encrypt the first 10% of the file size
  - Files > 5MB and ≤ 20MB: For every 1/6th of the file size, encrypt the first 4KB
  - Files > 20MB: For every 10MB, encrypt the first 4KB

Features



Ransom Note



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

DEVMAN
Hello!

Your files have been stolen from your network and encrypted with a strong algorithm. We work for money and are not associated with politics.

--- Our communication process:

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

--- Client area (https://tox.chat):

>>> Contact this ID: C173B0BBD44655F3E0C2CD2FA721D24A72DE7BD5F51E2199594235BC097C25352E6C943C8F90

* If you prefer email - devman@cyberfear.com

--- Recommendations:

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.

--- Important:
If you refuse to pay or do not get in touch with us, we start publishing your files.
Ehe decryptor will be destroyed and the files will be published on our blog.

README.yAGRTb.txt

Extension

.yAGRTb

Production Language

C/C++

Figure 8. Overview of Devman Ransomware

Devman Ransomware Strategy

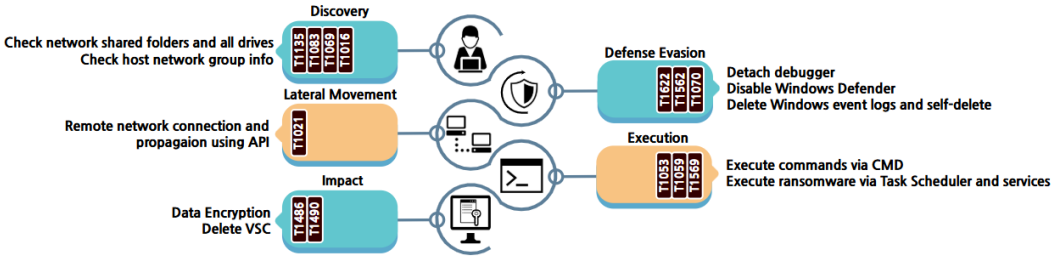


Figure 9. Devman Ransomware Attack Strategy

The Devman ransomware shares the majority of its functionalities with the Mamona ransomware. However, notable distinctions include the ability to change the icon to a specified image file, the addition of a feature to relaunch the ransomware for debugger separation, and significantly enhanced network propagation capabilities. These modifications are partially reflected in the execution parameters. In the Mamona version, the parameter -H, used to transmit the NTLM[3] hash for network authentication, has been removed in the Devman version. Additionally, new parameters have been introduced: -ldap to activate network propagation, -host to specify network propagation targets, and -detached to disable the debugger separation feature.

Type	Description
-log	Log output
-keep	Self-deletion disabled
-skip-net	Encrypt local disks only
-skip-local	Encrypt network drives only
-code {32Bytes key}	Password required to execute ransomware
-sub {subnet}	Target network range for encryption
-p {password}	Network login password
-u {username}	Network login username
-time {HH:MM}	Execute after waiting until specified time (HH:MM)
-delay {ss}	Execute after waiting for specified duration
-threads {int}	Set number of encryption threads
-path {path}	Encrypt specified folders
-host {ip_addr}	**Encrypt specified hosts**
-ldap	**Enable network propagation**
-detached	**Disable ransomware re-execution**

Table 1. Execution Parameters of Devman Ransomware

[3] NTLM: An authentication protocol that uses password hashes instead of plaintext passwords to grant access.

The Devman ransomware, in addition to its execution parameters, securely encrypts and stores a variety of information within a specific session. This includes encryption-related configurations, the contents of the ransom note, and the public key necessary for key generation. It subsequently decrypts this information for use. The verified details are as follows.

Offset	Description
config[0]	Partial encryption ratio
config[4]	Ransom note content
config[2056]	Enable self-deletion
config[2057]	Enable event log deletion
config[2058]	Enable service termination
config[2059]	Enable process termination
config[2060]	Enable password verification
config[2061]	Encryption mode
config[2062]	Enable ransom note printing
config[2064]	Enable icon change
config[2065]	Enable network share mounting
config[2066]	Ransomware password (32 bytes)
config[2098]	Encrypted file extension
config[2114]	Curve25519 public key (32 bytes)

Table 2. Configuration Parameters of Devman Ransomware

Ransomware also engages in the deletion of various records and traces to thwart recovery efforts and impede analysis. It completely erases data in the recycle bin and, depending on the configuration settings, deletes all event logs within the Windows environment. Furthermore, it utilizes command prompt commands to remove backup copies, and once the encryption of all files is complete, the ransomware autonomously deletes itself.

Command	Description
cmd.exe /c vssadmin delete shadows /all /quiet	VSS deletion
cmd.exe /C ping 127.0.0.7 -n 3 > Nul & Del /f /q \"%s\	Self-deletion

Table 3. Commands Related to Deletion

If the configuration settings include parameters related to the termination of services or processes, certain services and processes will be prioritized for termination to facilitate seamless file encryption. The services and processes targeted for termination are listed in the table below.

Service	Process
WinDefend, SecurityHealthService, wscsvc, Sense, WdNisSvc, WdNisDrv, WdFilter, WdBoot, wdnisdrv, wdfilter, wdboot, mpssvc, mpsdrv, BFE, MsMpSvc, SepMasterService, wscsvc, SgrmBroker, SgrmAgent, EventLog	MsMpEng.exe, NisSrv.exe, SecurityHealthService.exe, smartscreen.exe, SecHealthUI.exe, MpCmdRun.exe, MSASCui.exe, MpUXSrv.exe, SgrmBroker.exe, MsSense.exe, SenseIR.exe, SenseCE.exe, SenseSampleUploader.exe, SenseNdr.exe,

Table 4. Target Services and Processes for Termination

After terminating services and processes, the ransomware propagates across the network. This execution requires the use of the -ldap parameter, and additionally, propagation can be attempted to specific hosts using the -host parameter or to all hosts within a particular subnet range using the -sub parameter. In previous versions of Mamona, network connections are attempted via IPC$ [4], necessitating the input of login credentials, an authentication NTLM hash, and a login password through the -u, -H, and -p parameters, respectively. Although the -H parameter receives the hash value for authentication, actual NTLM authentication is not conducted; instead, login attempts are made using the -u and -p parameters. If access is granted, the method employed encrypts files located in the network's shared resources without further propagation of the ransomware.

```
  if ( log_flag )
  {
    print_log_sub_402730(Format: L"attempting hash auth to %s with user %s", v10, v11 + 568);
    v13 = v11 + 1608;
  }
  if ( !auth_ntlm_sub_406570(v10, lpUserName: (v11 + 568), v13) )
  {
    if ( log_flag )
      print_log_sub_402730(Format: L"hash auth failed, trying password auth");
LABEL_20:
    lpUserName = (v11 + 568);
    if ( !*(v11 + 568) || (lpPassword = (v11 + 1088), !*lpPassword) )
    {
      lpPassword = 0;
      lpUserName = 0;
    }
    if ( WNetAddConnection2W(lpNetResource: &cp, lpPassword: lpPassword, lpUserName: lpUserName, dwFlags: 0) )
      return HeapFree_wrp(lpMem: *(v1 + 4));
    WNetCancelConnection2W(lpName: Name, dwFlags: 0, fForce: 1);
  }
  if ( log_flag )
    print_log_sub_402730(Format: L"found accessible host: %s", *(v1 + 4));
```

Figure 10. Network Authentication Method of Mamona Ransomware

[4] IPC$: shared folder used for authentication when accessing another computer over a network.

In the case of the Devman ransomware, rather than attempting network encryption through IPC$, it employs a method of propagation utilizing LDAP[5]. If the login ID provided via the -u parameter is in the form of id@domain, it extracts the domain information from this and uses it to retrieve information on all hosts connected to the Active Directory (AD)[6]. Subsequently, it verifies whether authentication is possible on each host using the ID from the -u parameter and the password from the -p parameter. Once authentication is confirmed, the ransomware is disseminated across all authenticated hosts.

```
vsprintf_sub_409070(NewFileName, 260, L"%s\\Temp\\cleanup.exe", Name);
NetResource.dwType = 1;
NetResource.dwScope = 0;
memset(&NetResource.dwDisplayType, 0, 12);
NetResource.lpComment = 0;
NetResource.lpProvider = 0;
NetResource.lpRemoteName = Name;
if ( log_flag )
  print_log_sub_409040("[+] Connecting to share: %ws\n", Name);
v6 = WNetAddConnection2W(lpNetResource: &NetResource, lpPassword: lpPassword, lpUserName: lpUserName, dwFlags: 0);
if ( v6 )
{
  if ( log_flag )
    print_log_sub_409040("[!] Failed to connect to share: %ws (Error: %d)\n", Name, v6);
  return 0;
}
if ( log_flag )
  print_log_sub_409040("[+] Connected to share, copying binary\n");
if ( CopyFileW(lpExistingFileName: Filename, lpNewFileName: NewFileName, bFailIfExists: 0) )
{
  TickCount = GetTickCount();
  vsprintf_sub_409070(sc_name, 32, L"Radio_%d", TickCount);
  vsprintf_sub_409070(
    CommandLine,
    520,
    L"sc \\\\%s create %s binPath= \"%%windir%%\\Temp\\cleanup.exe %s\" start= demand",
```

Figure 11. Propagation and Execution of Devman Ransomware

The ransomware replicates itself under the filename cleanup.exe in the temporary folder of the connected host, subsequently registering as a service or executing via the task scheduler. Additionally, to prevent multiple propagation attempts within the same network, the ransomware is executed on remote hosts with the inclusion of the -skip-net argument. The command utilized is detailed in the table below.

Command	Description
sc \\{host_ip} create Radio_[0-9]{32} binPath= "%%windir%%\\Temp\\cleanup.exe -skip-net" start= demand	Create service on remote host
sc \\{host_ip} start Radio_[0-9]{32}	Start service
schtasks /create /s {host_ip} /u {username} /p {password} /tn "CoolTask" /tr "%%windir%%\Temp\cleanup.exe -skip-net" /sc once /st 00:00	Create scheduled task
schtasks /run /s {host_ip} /u {username} /p {password} /tn	Execute scheduled task
schtasks /delete /s {host_ip} /u {username} /p {password} /tn	Delete scheduled task

Table 5. Target Services and Processes for Termination

[5] LDAP: A protocol for storing and retrieving data such as users, groups, devices, and credentials over a network.

[6] AD (Active Directory): Windows LDAP-based directory system that enables centralized management of users and computers.

Following the propagation across the network, the encryption of the local system is initiated. By employing the -skip-local parameter, only network shared folders are encrypted, whereas the -skip-net parameter restricts encryption to local disks alone. Furthermore, utilizing the -path argument allows for the encryption of specific directories and their subdirectories exclusively. Once the encryption targets have been designated, each directory is traversed to ascertain whether it corresponds to any exception items. Apart from the addition of the .bin extension to the exception list in the Devman version, the encryption exceptions remain consistent across both versions. The encryption exception targets are delineated in the table below.

Folder name	File extension, and File name
Windows, Program Files, Program Files (x86), AppData, ProgramData, All Users, NETLOGON, SYSVOL	PrintMe22.pdf, .exe, .dll, .msi, .sys, .ini, .ink, .bin

Table 6. Subjects of Encryption Exceptions

The file encryption methodology is delineated into two distinct encryption modes, contingent upon the configuration settings. These settings encompass two pivotal options: one that determines the encryption mode and another that dictates the partial encryption ratio. The first method pertains to the encryption of only the initial segment of large files. Files that are 1MB or smaller undergo full encryption, while those up to 5MB in size have only the first 1MB encrypted. For files exceeding 5MB, the encryption process involves encrypting only the initial portion of the file, as specified by the attacker's designated ratio, with the encrypted segment being capped at a maximum of 70MB.

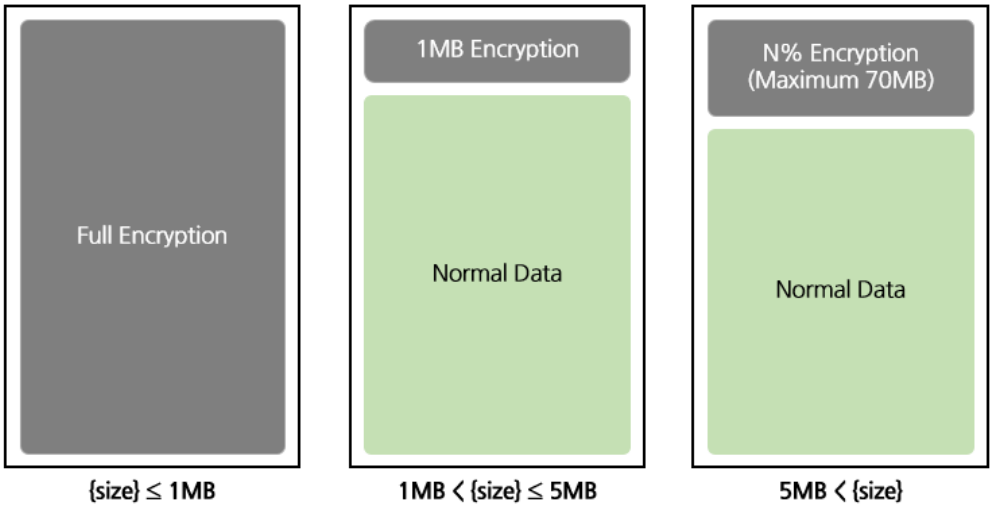


Figure 12. File Encryption Methods by Size - 1

The second method involves encrypting files at regular intervals, particularly for those of substantial size. Files that are 64 bytes or smaller undergo full encryption. For files up to 5MB, only 10% of the total size is encrypted. Files that are 20MB or smaller are divided into segments equivalent to one-sixth of the total size, with only the first 4KB of each segment being encrypted. For files exceeding 20MB, the first 4KB is encrypted for every 10MB segment.

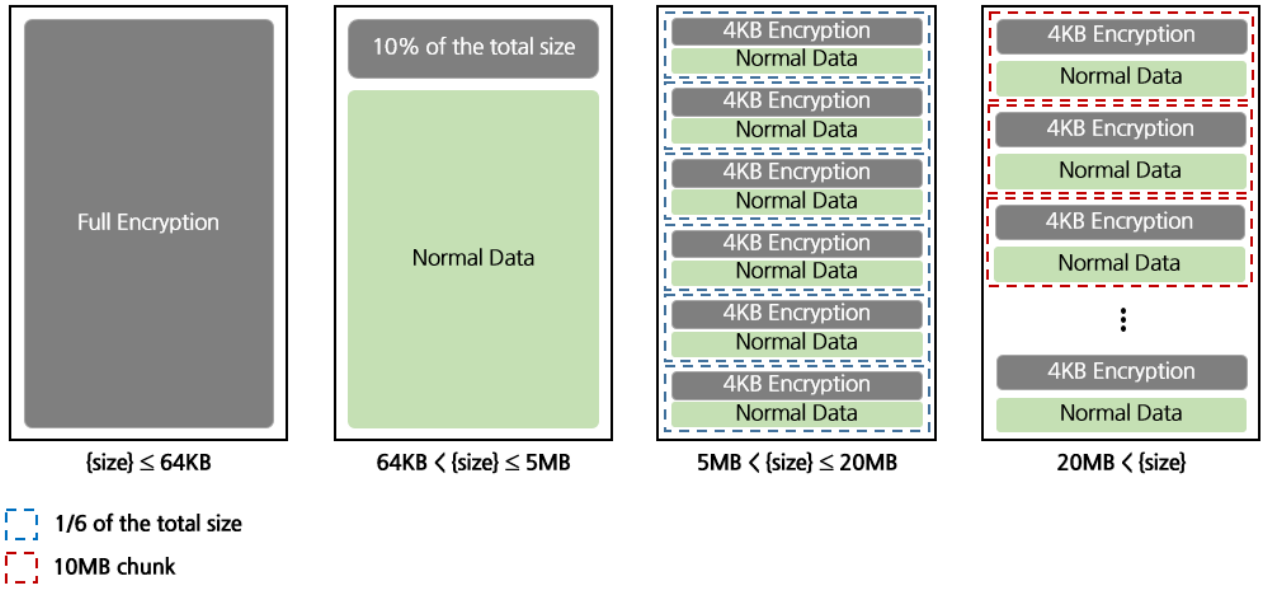


Figure 13. File Encryption Methods by Size - 2

Both encryption methods employ the same algorithm, utilizing a shared secret generated via Curve25519 for the encryption key. For each file, a random private key is generated, after which a shared secret can be established using the hardcoded public key of Devman. This process exploits the property of Curve25519, where the shared secret derived from one's private key and the counterpart's public key is identical to the shared secret obtained from one's public key and the counterpart's private key. The shared secret is then hashed using the SHA-512 algorithm, and the last 32 bytes of the hash are employed as the key for encrypting the file with the HC-128 algorithm. At the end of the file, the Curve25519 public key necessary for key recovery is stored.

Upon the completion of file encryption, a ransom note is generated in each designated encryption path. If the option to print the ransom note is enabled, the contents of the ransom note are saved in PDF format and subsequently printed on all connected printers. The ransom note is stored in the temporary folder under the name PrintMe22.pdf.

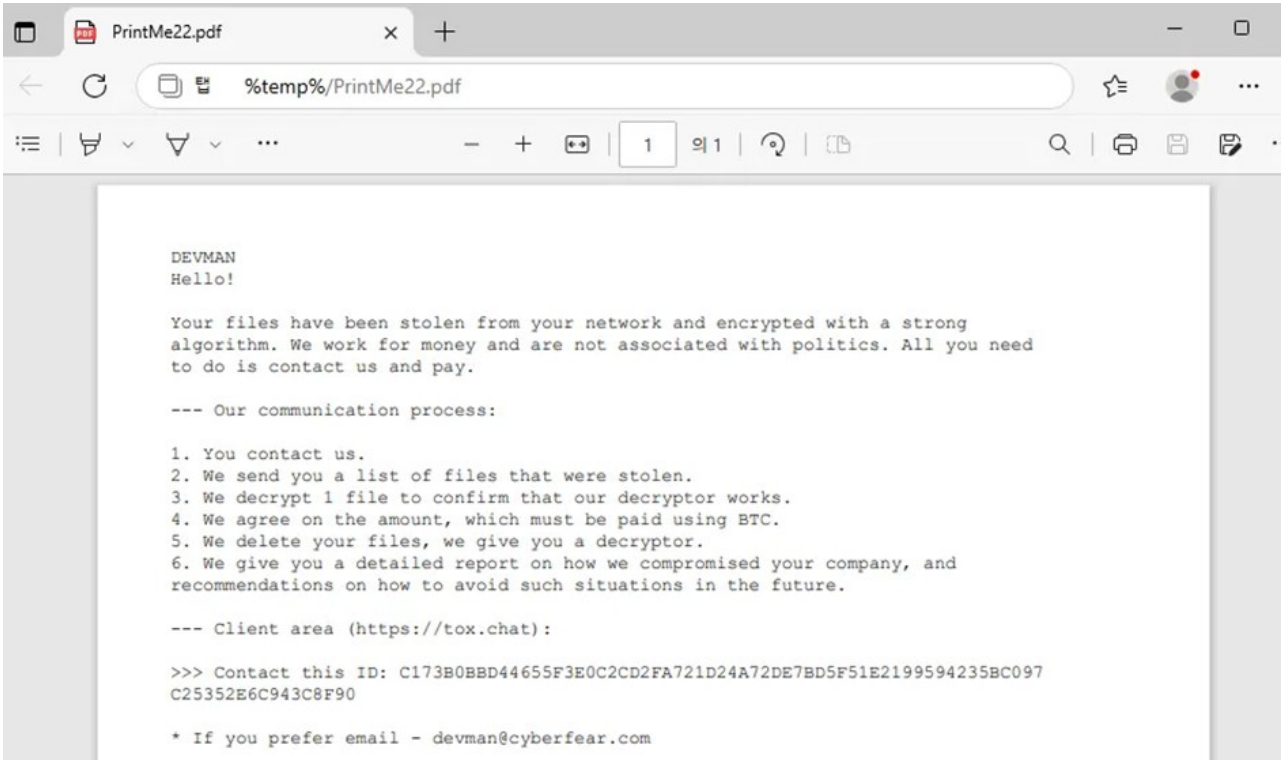


Figure 14. Ransom Note for Output

Furthermore, to alter the icons of encrypted files, the icon image file, stored in Base64 format, is temporarily saved in a designated folder. Subsequently, the registry settings are modified to arbitrarily change the icon. Additionally, the desktop wallpaper is altered to an image displaying the message, "YOUR FILES HAVE BEEN ENCRYPTED! CHECK README.yAGRTb.txt."

Figure 15. Altered Desktop Background

Response Strategies for DragonForce Ransomware

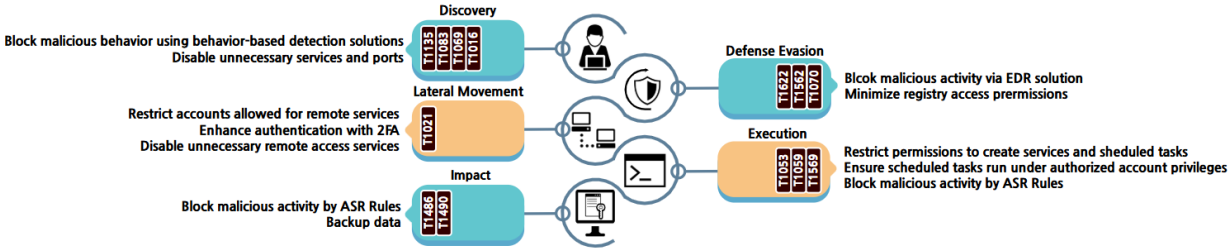


Figure 16. Countermeasures for Devman Ransomware

The Devman ransomware exploits various types of information, such as network shared folders and the domain to which a system belongs, to encrypt files and propagate across networks. Consequently, it is possible to thwart malicious activities by employing behavior-based detection solutions. Additionally, by eliminating or deactivating unnecessary network services, one can prevent the dissemination of damage across the network.

To evade detection of its malicious activities, ransomware disables Windows Defender, detaches debuggers, and deletes various event logs. Utilizing an Endpoint Detection and Response (EDR)[7] solution can effectively block such malicious actions as the deactivation of Windows Defender and the deletion of event logs. In particular, the deletion of event logs necessitates access to the registry; by minimizing registry access permissions, one can prevent attackers from arbitrarily deleting event logs.

Furthermore, in an attempt to disseminate ransomware within the network environment, there are efforts to gain access using login IDs and passwords. Although there has been no verified process for the collection of these IDs and passwords, it is plausible that during the preparatory phase of the attack, account information could be gathered, leaked, or exploited, particularly if the accounts are vulnerable. Consequently, it is imperative to fortify authentication mechanisms by employing two-factor authentication (2FA)[8]. Additionally, restricting accounts that can utilize remote services or deactivating unnecessary remote services altogether can serve as a deterrent, effectively preventing attackers from infiltrating the network environment.

[7] EDR (Endpoint Detection and Response): A real-time solution for detecting and mitigating malicious behavior on endpoints like computers, mobile devices, and servers.

[8] 2FA (2-factor Authentication): An authentication method that adds a second factor, such as a mobile device or OTP, in addition to ID and password.

The aforementioned malicious activities predominantly exploit the Windows Command Prompt or are executed through the registration of tasks and services. Consequently, by activating ASR (Attack Surface Reduction)[9] rules, one can effectively intercept and prevent such anomalous processes, thereby thwarting malicious actions. Furthermore, given that ransomware often stores its programs in temporary folders or replicates itself in specific locations for task registration, it is feasible to employ Anti-Virus solutions to isolate suspicious files. Additionally, it is imperative to restrict the creation permissions for services and task schedulers to prevent the remotely executed replication of ransomware. Even if scheduled tasks are executed, configuring them to run under the authority of authenticated accounts can significantly mitigate potential damage.

To prevent users from arbitrarily recovering encrypted files, all backup copies present within the system are deleted prior to file encryption. By activating ASR (Attack Surface Reduction) rules, it is possible to block processes that delete backup copies and encrypt files. Moreover, it is imperative to implement measures such as dispersing backup copies to separate networks or storage locations, ensuring recovery is feasible even if the system undergoes encryption.

[9] ASR (Attack Surface Reduction): A protection feature that blocks specific processes and executables used by attackers.

Indicators of Compromise (IoCs)

Hash(SHA-256)
1f6640102f6472523830d69630def669dc3433bbb1c0e6183458bd792d420f8e
c5f49c0f566a114b529138f8bd222865c9fa9fa95f96ec1ded50700764a1d4e7

■ Reference Websites

• GMA Network (https://www.gmanetwork.com/news/topstories/nation/945481/gma-network-statement-on-cybersecurity-incident)

• RELIAQUEST (https://reliaquest.com/blog/threat-spotlight-reliaquest-uncovers-vulnerability-behind-sap-netweaver-compromise/)

Special Report

Zero Trust Security Strategy: Devices and Endpoints

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

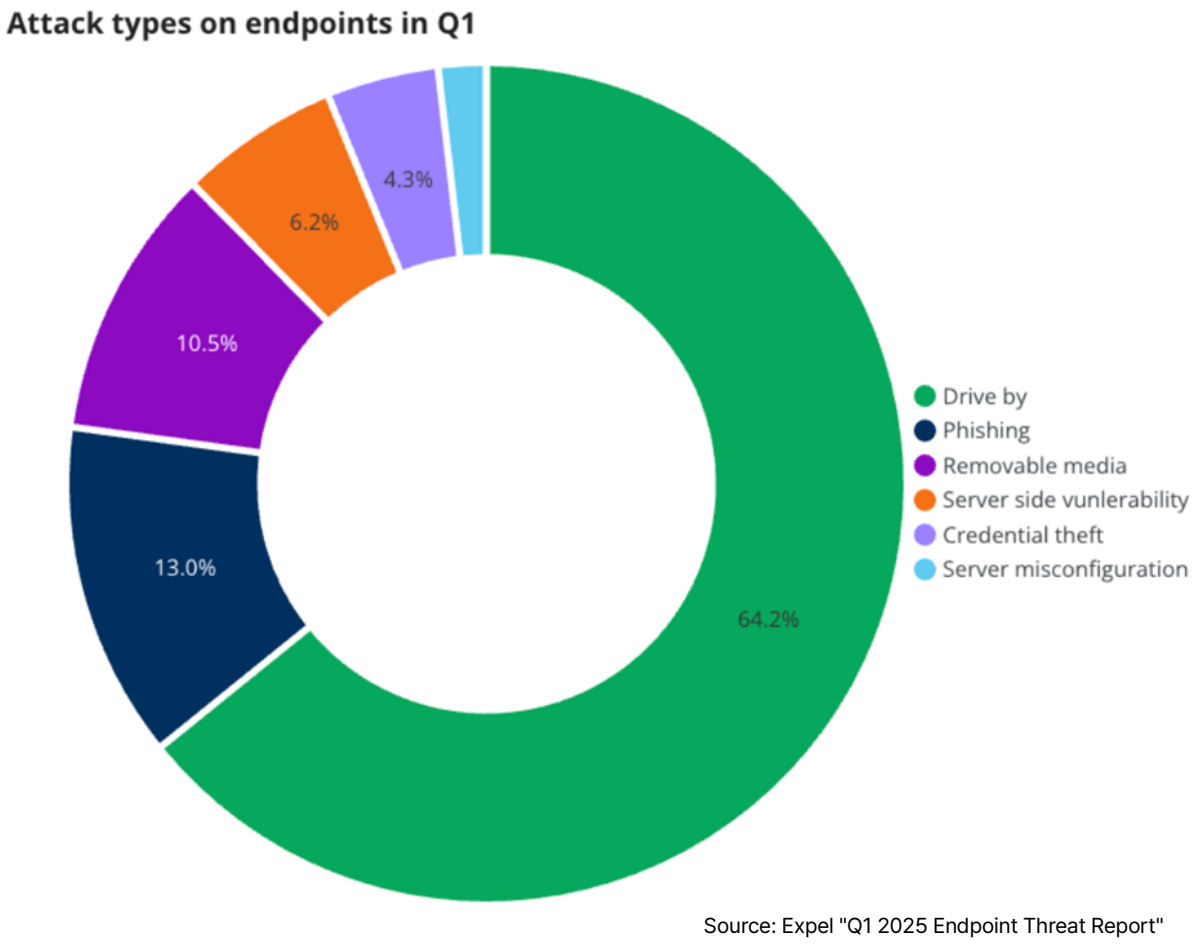
■ Overview of Device and Endpoint Pillars

In a Zero Trust Architecture, the Device and Endpoint pillar is intricately linked with the Identity pillar, functioning as a critical control point that determines final access based on the device's status and security trustworthiness before a user gains access to sensitive resources. Even if a user's identity is authenticated, access must be restricted if the device is unverified or fails to meet security standards. This underscores the necessity of implementing a framework, as emphasized in CISA's guidelines, that dynamically adjusts access policies based on a multitude of factors, including the status, location, and behavior of both the user and the device.

Since the onset of the COVID-19 pandemic, the work environment has undergone a rapid transformation. Consequently, critical organizational information has transitioned to a form where it is distributed and utilized across a variety of devices that users employ in their daily routines, such as personal computers, laptops, and tablets. These devices traverse multiple security perimeters, connecting to internal networks, external networks, and cloud environments. This is particularly evident as remote work, business trips, and external client meetings have led to the frequent use of both company-owned and personally-owned devices (BYOD) in public spaces or on external networks.

In the domestic context, the traditional security infrastructure, predominantly designed around physical network separation, is increasingly becoming a structural constraint due to the expansion of remote and flexible work arrangements. To address this issue, initiatives such as the National Intelligence Service-led 'National Network Security Framework Guidelines (N2SF)' and the Financial Services Commission's 'Roadmap for Improvement of Network Separation in the Financial Sector' propose a phased relaxation of network separation environments alongside the implementation of zero-trust-based supplementary measures. This trend necessitates a more sophisticated approach to security verification and control mechanisms at the device and endpoint levels.

With the diversification of devices and endpoint environments, attacks targeting endpoints have been on a steady rise. According to the recent "Q1 2025 Endpoint Threat Report" by Expel, 68% of all security incidents targeting organizations occurred at endpoints. The accompanying illustration delineates a variety of attack vectors, including drive-by downloads, phishing, removable media, and server-side vulnerabilities. Notably, drive-by attacks constituted the majority, accounting for 64.2% of all endpoint attacks, underscoring the limitations of relying solely on traditional network-centric passive defenses.



Source: Expel "Q1 2025 Endpoint Threat Report"

Figure 1. Types of Endpoint Attacks in the First Quarter of 2025

"In global reports such as those from Expel and CrowdStrike, the term 'devices and endpoints' often encompasses systems, including servers. However, within the context of domestic zero-trust practices, it is imperative to interpret this from an endpoint perspective that primarily focuses on user devices."

As threats to devices and endpoints become increasingly sophisticated and intelligent, relying solely on traditional firewall and antivirus-centric responses is insufficient. A multi-layered defense system is imperative, incorporating a diverse array of response strategies such as behavior-based detection (EDR/XDR), Unified Endpoint Management (UEM), continuous security posture monitoring, and policy-based access control. From a zero-trust perspective, the dynamic assessment of the trustworthiness of devices and endpoints, alongside the real-time detection and mitigation of threats, is paramount in establishing an effective security framework.

In a zero-trust environment, it is imperative to not only verify the identity of the user but also to concurrently assess the reliability and security status of the device from which the user is attempting to gain access. For instance, even if users possess identical credentials, access to critical systems or data within the enterprise must be automatically restricted if the device in question is unauthorized or deemed high-risk, such as those lacking necessary patches, infected with malware, or exhibiting anomalous behavior. This interconnected control of identifiers and device pillars ensures that sensitive assets within the organization are substantively safeguarded, thereby playing a decisive role in mitigating the vulnerabilities inherent in single authentication frameworks.

Within the Zero Trust Architecture, devices and endpoint fillers transcend their role as mere access conduits, functioning instead as pivotal axes in organizational access policies and real-time risk assessment. Particularly, given that devices serve as the tangible access entities utilized by actual users in their professional activities, their role as a Policy Information Point (PIP) is underscored. This involves providing various attribute information and security status during the policy decision-making process.

Consequently, when enhancing the device and endpoint domains from the perspective of a Zero Trust Architecture, organizations can not only effectively counter increasingly sophisticated threats but also establish a foundation for securely safeguarding critical assets and information.

■ Key Elements of the Device/Endpoint Pillar

Devices and endpoint pillars, alongside user identity, constitute a critical security control domain within a zero-trust architecture, applied at the preliminary stage of actual resource access. Devices serve as the tangible interface utilized by users in their professional activities and represent the juncture at which a myriad of threats to organizational assets and data materialize in reality.

In particular, within a zero-trust environment, all devices and endpoints are regarded as untrustworthy entities, necessitating real-time verification and the application of granular policies based on the device's status, trustworthiness, and risk level. To achieve this, an integrated management framework encompassing various elements such as device inventory (asset cataloging), device authentication, BYOD management, vulnerability and patch management, and risk assessment must be established.

The following section delves into the principal components of device and endpoint pillars, along with a detailed examination of the administrative and technical strategies essential for their implementation.

1. Device Inventory

In a Zero Trust environment, the device inventory serves as the foundational framework for systematically identifying and managing all devices that have access to organizational resources. The scope of management extends beyond desktops, laptops, smartphones, and tablets to include IoT devices, printers, and portable storage devices. Consequently, organizations must establish identification policies based on detailed attributes such as device type, operating system, and hardware and software characteristics. Furthermore, it is imperative to manage various inventory information in an integrated manner.

The device inventory encompasses not merely a simple cataloging but extends to the automatic registration of newly connected devices to the network, as well as lifecycle management including changes in device status, relocation, and decommissioning. It is imperative to maintain the accuracy and currency of inventory information by integrating with automated asset management systems, Unified Endpoint Management (UEM), Active Directory (AD), and similar platforms.

The registered inventory information encompasses a wide array of data, including the owner, affiliated department, purpose, security classification, and connection history. This information serves as pivotal resources for the enforcement of security policies, anomaly detection, and incident response. Furthermore, devices can be categorized based on factors such as importance, risk level, and type of operation, allowing for differentiated access control and security policies to be applied to each group. For instance, by distinguishing between management devices, general user devices, and those belonging to external partners, it becomes feasible to effectively control the unnecessary proliferation of privileges and mitigate internal threats.

2. Device Authentication

In a Zero Trust environment, device authentication transcends the mere acknowledgment of a device's registration status. Organizations are compelled to ascertain the trustworthiness of each device making access requests by leveraging unique identification information, such as MAC addresses, digital certificates, and serial numbers. This verification process must be complemented by cross-referencing not only authentication data but also the owner, registration history, and management status of the device. It is imperative to design policies that fundamentally block network access for unauthorized and unapproved devices, thereby ensuring robust security measures are in place.

Device authentication should not remain a one-time procedure. Organizations must periodically conduct comprehensive trust assessments by evaluating a multitude of factors, including the device's network connectivity status, the currency of its operating system and software updates, its physical location, the user's access history, and behavioral patterns. For instance, in scenarios where unpatched devices, malware infections, or access from anomalous locations and times are detected, it is imperative to implement additional procedures such as supplementary authentication or access restrictions. The efficacy of these trust assessments is significantly enhanced when integrated and automated in real-time with security systems such as Unified Endpoint Management (UEM) and Endpoint Detection and Response (EDR).

Based on the results of device trustworthiness assessments, organizations must establish granular response policies for each device, encompassing access permissions, restrictions, isolation, and additional authentication measures. For devices with low trust ratings, it is imperative to consider automatically blocking access to sensitive assets or transferring them to a separate management framework. All these processes should be integrated with security policies through a unified operational framework that includes ICAM (Identity, Credential, and Access Management), SSO (Single Sign-On), EDR (Endpoint Detection and Response), and UEM (Unified Endpoint Management). This integration is essential to enhance the organization's overall risk response capabilities.

3. Management of BYOD (Bring Your Own Device)

In a Zero Trust environment, the management of Bring Your Own Device (BYOD) necessitates that while individuals are permitted to access organizational resources using personally owned devices such as laptops, smartphones, and tablets for work purposes, this access must be accompanied by stringent security controls and adherence to policies. Conducting work through personal devices can significantly enhance user convenience and productivity; however, it simultaneously perpetuates the potential risk of exposing the organization's sensitive information to external environments.

Therefore, organizations must explicitly delineate their policies regarding the adoption of BYOD, including the scope of its allowance, approval procedures, security standards, operating systems, and management platforms (MDM/UEM). It is crucial to establish detailed criteria concerning the types of devices permitted, platforms, software lists, and the mandatory installation of security applications.

The BYOD policy must incorporate a diverse array of security requirements, including device registration, periodic security status assessments, access history logging, enhanced authentication such as Multi-Factor Authentication (MFA) for access to critical resources, and the segregation of cloud and network environments. Furthermore, it is imperative to address the protection of personal data and the prevention of privacy infringement for BYOD users. To this end, procedures must be established to provide users with prior notification and obtain their consent regarding the minimum scope and purpose of monitoring, as well as the information accessible.

The risk assessment of BYOD (Bring Your Own Device) should be conducted periodically, comprehensively reflecting factors such as the security status of the device, OS vulnerabilities, malware infection status, the presence of antivirus or MDM (Mobile Device Management) installations, and any history of policy violations. It is efficient to automate such assessments through integrated management solutions like UEM (Unified Endpoint Management), MDM, and EDR (Endpoint Detection and Response). Devices assessed with high risk can be managed with differentiated response policies, such as restricting access to sensitive data, requiring additional authentication, or isolating them from the organization's network.

Real-time monitoring within a BYOD (Bring Your Own Device) environment is equally indispensable. The management system should be configured to collect and analyze a wide array of elements, not only encompassing fundamental information such as the operating system, manufacturer, installation details, software, and network access history, but also extending to the detection of BYOD policy violations, abnormal access patterns, and automatic alerts upon the occurrence of suspicious activities. When monitoring BYOD, it is imperative to ensure that the principle of logical separation between work-related data and personal data is strictly upheld, so as to prevent any disruption of business operations or excessive invasion of privacy.

4. Device Vulnerability Management

In a Zero Trust environment, device vulnerability management transcends the mere application of the latest patches for software or operating systems. It must encompass the entire lifecycle, including the detection of vulnerabilities, impact assessment, and prompt response for all devices within the organization, such as PCs, laptops, mobile devices, and IoT devices.

First and foremost, organizations must establish a regular and systematic policy for the identification and assessment of vulnerabilities. This policy should meticulously outline a comprehensive management framework, which includes procedures for diagnosing vulnerabilities specific to each device, evaluation criteria, automated inspection intervals, and a process for taking corrective action upon the discovery of vulnerabilities.

During the vulnerability assessment phase, security systems such as Unified Endpoint Management (UEM), Mobile Device Management (MDM), and Endpoint Detection and Response (EDR) are employed to conduct periodic scans of all devices connected to the network. This process involves identifying a myriad of vulnerabilities, including unpatched operating systems, insecure applications, and unnecessary running services. It is imperative that swift actions are taken based on the risk classification and prioritization of these vulnerabilities. It is advisable to concurrently implement automated responses such as deploying the latest security patches, removing vulnerable software, altering configurations, and isolating networks.

Upon the identification of vulnerabilities, it is imperative to conduct a thorough analysis of their potential impact and exploitability, subsequently formulating a response strategy prioritized accordingly. For instance, vulnerabilities that pose a significant risk of tangible damage, such as breaches of critical internal systems, data exfiltration, or ransomware infections, necessitate the immediate implementation of robust countermeasures, including blocking, patching, and isolation. The results of the vulnerability impact analysis, along with the response procedures, should be meticulously documented in a separate report, serving as a rapid reference resource in the event of similar threats in the future.

The results of vulnerability management can be directly incorporated into 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 segregation, thereby effectively mitigating tangible risks.

Comprehensively, the device vulnerability management system serves as a foundation for consistently maintaining the security level of all terminals within an organization and proactively mitigating the potential for security breaches. This is achieved by integrating it with device inventory, authentication, and trust evaluation processes.

5. Device Patch Management

In a zero-trust environment, device patch management is a pivotal element in consistently maintaining the security level of all devices within an organization. Patch management transcends mere software updates; it necessitates the establishment of systematic policies, the definition of procedures, and the implementation of a comprehensive management framework that encompasses the entire lifecycle, including patch deployment, verification, and post-deployment management.

Organizations must first establish a patch management policy that meticulously delineates the principles and procedures for applying patches to device operating systems, applications utilized within devices, firmware, and other relevant components. This policy should encompass critical elements such as the cataloging of devices under management, the prioritization of patches, the processes for patch distribution and installation, backup and recovery strategies, and the management of patch application history. It is imperative that the patch management policy is regularly reviewed and updated to reflect changes in the actual security environment and advancements in technology.

When deploying patches, it is imperative to comprehensively consider the characteristics of each device, the operational environment, and the criticality of tasks, while actively leveraging automated systems such as Active Directory (AD) and Patch Management Systems (PMS). Rather than employing a uniform application approach across all endpoints, it is more efficacious to incorporate flexibility in the deployment schedule and methodology, taking into account the network environment, user convenience, and the impact on business operations. The design should be oriented towards ensuring that the latest patches are applied swiftly and without omission, using metrics such as accuracy, completeness, consistency, and scalability as management indicators.

Following the application of patches, it is imperative to establish a system capable of real-time monitoring of installation status and identifying any omissions. For patches that are either missing or have failed, it is advisable to promptly undertake supplementary actions. Furthermore, exceptional circumstances or failure histories should be managed through a distinct reporting mechanism. Additionally, the outcomes and records of patch management must be systematically documented and preserved to facilitate their proactive utilization in regular security audits, risk assessments, internal and external audits, and regulatory compliance.

Device patch management serves as the foundation for proactively mitigating security vulnerabilities across all endpoints within an organization and maintaining a consistent level of security. This is achieved by integrating it with device inventory, vulnerability assessment, and reliability evaluation.

6. Device Risk Management

In a Zero Trust architecture, device risk management is fundamentally aimed at safeguarding all operational devices within an organization from both physical and logical threats. Devices are susceptible not only to direct physical threats such as loss, theft, hijacking, and unauthorized access, but also to a myriad of risks including insider threats, malware infections, and data breaches.

Firstly, it is imperative that all devices are registered within an asset inventory to systematically manage critical information such as ownership, location, and usage history. To mitigate risks associated with physical loss or theft, physical security measures, such as locks, should be implemented on key equipment like laptops and tablets. For devices that are frequently moved, it is essential to establish immediate response systems, including GPS-based location tracking features and remote locking or data wiping capabilities in the event of loss.

Device users must be well-versed in the procedures for promptly reporting incidents such as loss or theft to the organization's IT personnel or security managers. To facilitate this, the organization is obligated to provide regular security training sessions and comprehensive guidelines.

Based on this multi-layered management and operational framework, organizations must implement an integrated security environment that does not solely rely on technical safeguards but also incorporates people, policies, and processes. Device risk management, consequently, serves as the foundation for minimizing a variety of risks such as information leakage, asset loss, and insider threats, while substantively enhancing business continuity and the level of information protection.

7. Unified Endpoint Management (UEM)

As the endpoint environment within organizations diversifies to include PCs, laptops, mobile devices, and IoT, Unified Endpoint Management (UEM) must comprehensively support the registration, authentication, policy deployment, security management, and data protection of various devices through a single platform. Evolving from the traditional Mobile Device Management (MDM), which primarily focused on the remote control of mobile terminals, the core objective now is to pursue consistent security policies and operational efficiency across all endpoints in the workplace.

The UEM policy must be intricately aligned with the organization's information protection guidelines and device management principles, encompassing detailed key security requirements such as device registration and authentication, access control, security threat detection and response, and data protection. In this context, UEM should not operate in isolation but rather in conjunction with ICAM, integrated monitoring systems, and other frameworks, thereby serving as a practical implementation platform for a zero-trust security architecture within the organization's device domain.

From the perspective of access control, Unified Endpoint Management (UEM) must meticulously manage the pathways and levels at which each device accesses organizational resources. In conjunction with network-based access control, policies such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) can be implemented through Identity, Credential, and Access Management (ICAM) integration. Furthermore, UEM should establish a dynamic and automated access control framework that incorporates user behavior analytics to impose specific restrictions or additional authentication procedures on devices identified as high-risk or exhibiting anomalous behavior.

Preventing data breaches is also a critical function of Unified Endpoint Management (UEM). Sensitive data within devices must be automatically identified and encrypted to ensure protection, and this should be integrated with Data Loss Prevention (DLP) capabilities to effectively block both intentional and unintentional data leaks. Organizations must regularly assess and enhance the effectiveness of their UEM policies and systems, continuously refining their management frameworks to proactively respond to new types of devices and emerging threats.

8. Endpoint Detection and Response (EDR) Expansion

The increasing sophistication of recent cyber threats has highlighted the limitations of relying solely on traditional signature-based security methods to detect and respond to all threats. Consequently, Endpoint Detection and Response (EDR) has emerged as a pivotal component in the security architecture of organizations' devices and endpoints. EDR employs a multi-layered approach, encompassing real-time detection, user behavior analytics, and continuous monitoring, to effectively safeguard against these advanced threats.

The real-time threat detection and prevention capabilities of Endpoint Detection and Response (EDR) systems are designed to swiftly identify a broad spectrum of threats, including various types of malware, insider threats, anonymous attacks, and social engineering-based intrusions. This is achieved by executing pre-configured countermeasures in accordance with automated policies. In this process, a combination of techniques such as behavior-based detection, file and network traffic analysis, and process monitoring is employed to establish a comprehensive response framework that addresses both known threats and previously unidentified attacks. Furthermore, upon threat detection, automated defensive actions—such as file deletion, network disconnection, and application execution restrictions—must be promptly implemented to mitigate potential damage.

An Endpoint Detection and Response (EDR) system must transcend mere threat detection by offering sophisticated capabilities that analyze endpoint user behavior and activities. After learning and defining normal usage patterns, the system should be capable of real-time detection of anomalous behaviors or signs of policy violations, thereby enabling immediate response upon the occurrence of any irregular activity. Through the granular collection of user-specific information and statistical analysis, the system can effectively address high-risk incidents such as potential insider threats or account takeovers.

Continuous device status monitoring is also a critical function of Endpoint Detection and Response (EDR). Rather than merely activating in response to threat occurrences, EDR must continuously monitor a diverse array of elements in real-time, including user behavior, system configurations, network access, and software installation statuses. This proactive surveillance is essential for the early detection of policy violations or exposure to vulnerabilities. The data collected, along with information on anomalous activities, is integrated with other security systems within the organization, such as Identity, Credential, and Access Management (ICAM) and unified monitoring systems. This integration forms the foundation for establishing a more comprehensive and rapid response framework.

9. Policies and Processes

To ensure the effective management and protection of devices and endpoints, the establishment of clear policies and a systematic management process is indispensable. Management policies based on the Zero Trust security model must encompass a wide array of management elements, including device approval procedures, inventory registration and onboarding, encryption scope and methods, regular backup and recovery, software management, security log monitoring, audits, and policy reviews. These elements should be concretized into detailed operational guidelines and execution procedures, necessitating systematic management to ensure consistent adherence by all members within the organization.

In particular, the management processes for devices and endpoints necessitate the establishment of a comprehensive, step-by-step management framework that encompasses the entire lifecycle of each device. This includes the introduction and deployment of new devices, maintaining security during usage, regular updates of operating software and vulnerability management, the return and disposal of devices post-use, and distinct procedures for external transfers or the use of portable media. For each of these stages, standardized operational processes must be developed. By instituting such processes, organizations can enhance their security posture, achieve real-time asset status monitoring, and facilitate the efficient allocation and operation of resources.

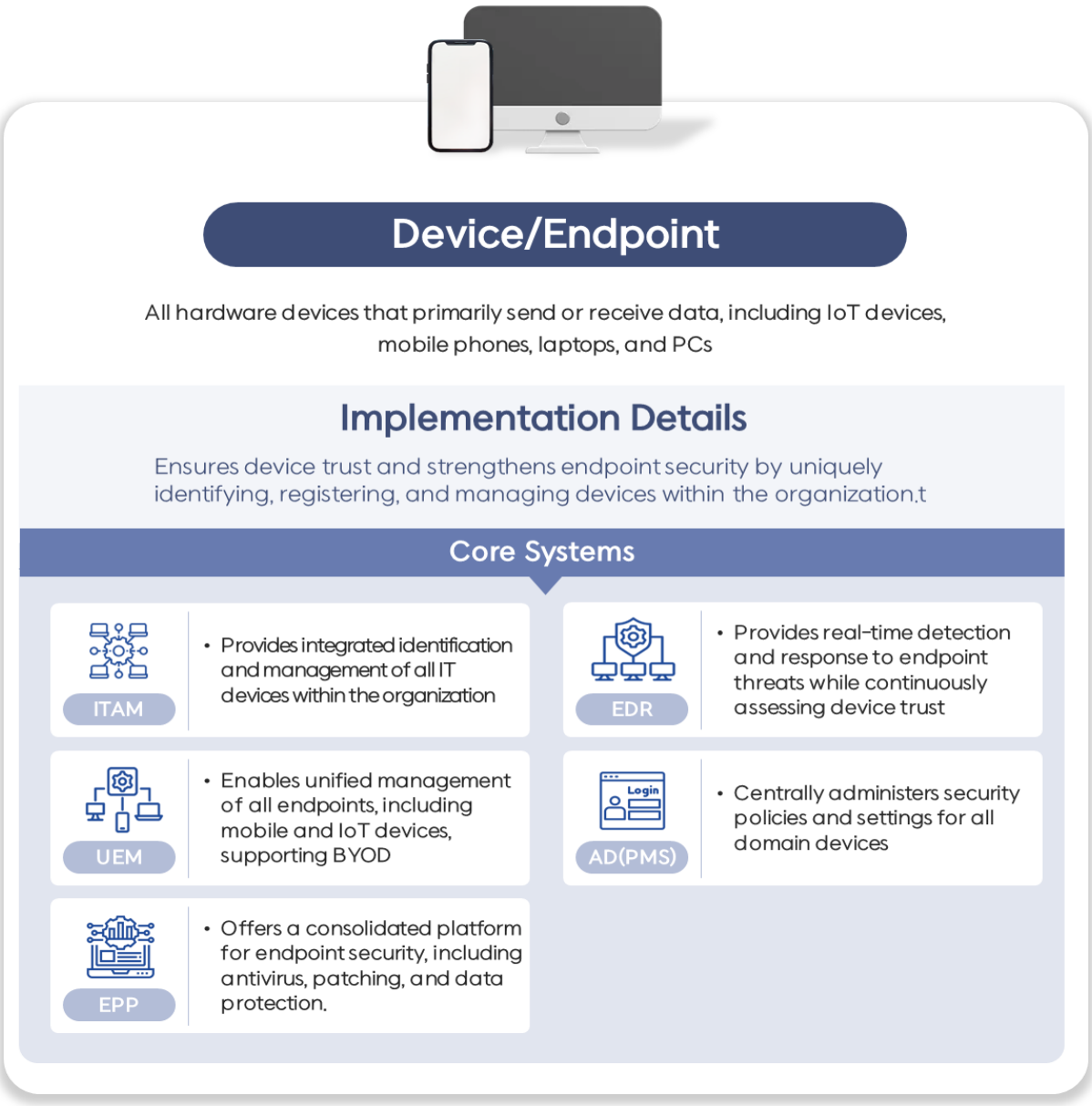
The refinement of policies and processes is an essential procedure for maintaining a consistent security posture across devices and endpoints, as well as for enabling swift risk response in an evolving work environment.

Based on these pivotal elements, the device and endpoint pillar serves as the practical security control axis of a Zero Trust Architecture. By meticulously managing the reliability and security status of all devices within an organization and verifying them in real-time, it ensures consistent control over not only the identity of users but also the risks associated with the devices utilized for actual access. This approach effectively safeguards critical assets from both internal and external threats, while offering 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 tangibly implemented.

■ Implementation of Zero Trust Features for Key Systems

To successfully implement a Zero Trust environment, it is imperative to have both technical solutions and the systems that execute them. The Zero Trust architecture is founded on the principle of "never trust, always verify." To realize this, systems must be in place to authenticate the identities of users and entities, continuously verify them, and ensure the enforcement of least privilege access.

The following key systems each play a pivotal role within a Zero Trust environment and are interconnected to bolster the organization's security posture. This analysis aims to delve into the specific functions that each system must perform to implement a Zero Trust environment and to examine the enhanced security benefits that the organization can attain as a result.



Source: SK Shields, "The Genesis of Zero Trust: Perfected with SKZT"

Figure 2. Primary Systems of Devices/Endpoints

1. ITAM (IT Asset Management)

The IT Asset Management (ITAM) system must function as both the starting point and foundational infrastructure for device and endpoint inventory within a Zero Trust Architecture. Organizations are required to establish a comprehensive management framework that encompasses the entire lifecycle of all IT and OA assets, including PCs, laptops, mobile devices, servers, printers, and IoT equipment. This framework should cover acquisition, registration, usage, relocation, decommissioning, and disposal. To ensure that asset information is accurately reflected in real-time, organizations must implement automated processes for registration, modification, and deletion. ITAM can be tailored and adopted through the customization of commercial solutions according to the specific operational environment of each organization or developed through in-house system integration (SI) efforts.

IT Asset Management (ITAM) systems must possess the capability to comprehensively manage a plethora of attribute information for each device. This includes asset numbers, barcodes, owners, affiliated departments, locations, purposes, operating systems, software installation statuses, security classifications, and connection histories. When new assets are introduced or when there are changes in status such as exportation or disposal, these changes must be automatically reflected in the inventory system. This ensures that the entire status can be comprehensively assessed at a glance, without any management gaps or information omissions. Particularly for devices with network access capabilities, the system should be able to automatically detect and block unregistered assets attempting to connect to the organization's network, or immediately notify security personnel of such events.

IT Asset Management (ITAM) must transcend its traditional asset management functionalities to seamlessly integrate with key security solutions such as Endpoint Detection and Response (EDR), Unified Endpoint Management (UEM), Active Directory (AD), Identity, Credential, and Access Management (ICAM), and Zero Trust Network Access (ZTNA). This integration is crucial for maintaining the currency and consistency of inventory information and for reflecting changes occurring in real-time within the actual network environment. The security status of each asset—such as patch application status, vulnerability assessment results, risk ratings, and access history—is continually updated through data exchanges between ITAM and security systems. Based on this updated information, dynamic policies can be applied, including device access control, isolation, and additional authentication measures.

In a Zero Trust environment, it is imperative to fundamentally block network access from unregistered devices. Furthermore, the flow of critical assets, including their introduction, removal, and disposal, must be meticulously tracked and recorded to facilitate audits and incident responses. Additionally, IT Asset Management (ITAM) should be integrated to ensure that security requirements are embedded throughout the entire asset lifecycle. This includes conducting basic security inspections upon asset introduction—such as initial state verification and malware detection—performing regular status checks during usage, and ensuring complete data erasure and retention of certification records upon asset removal or disposal.

Through IT Asset Management (ITAM), administrators can effortlessly discern the status of asset utilization, detect anomalies, and identify instances of security policy violations. This enables them to manage in real-time which devices are being operated, where within the organization, and for what purposes. The ITAM system must furnish a management environment endowed with precision, traceability, and reliability to promptly address a diverse array of requirements, including internal and external security audits, regulatory compliance, and breach incident analysis.

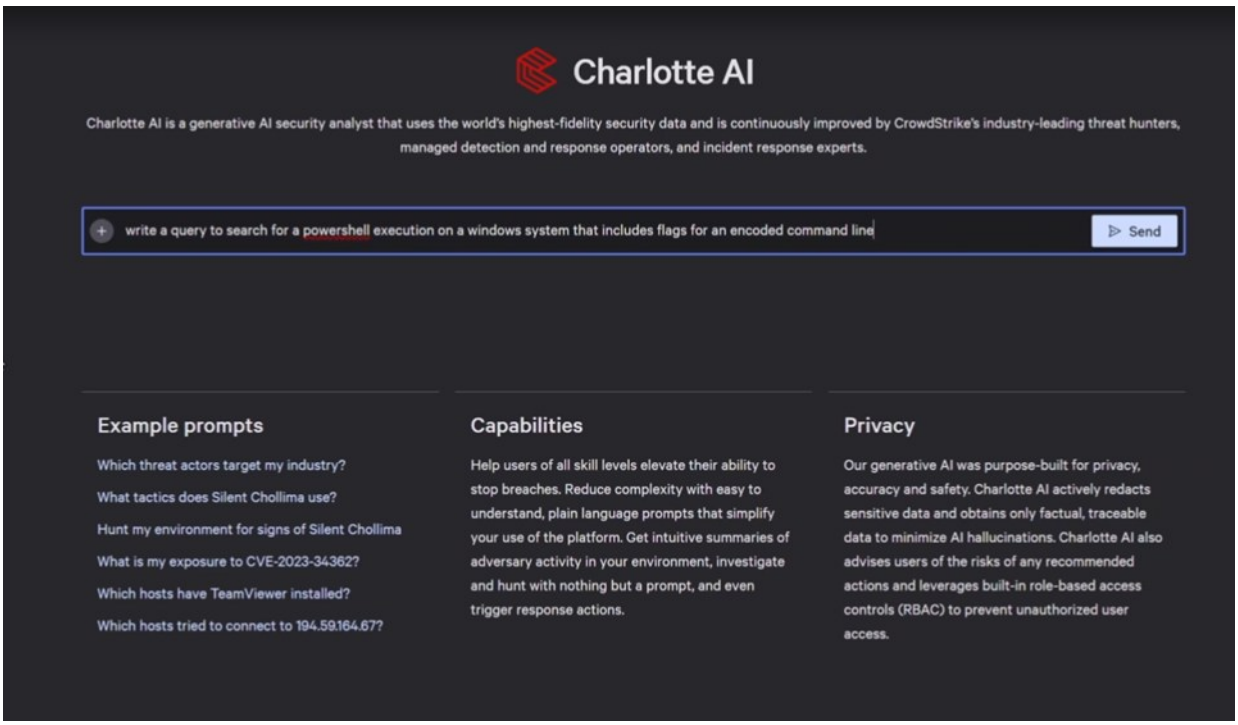
The advancement of IT Asset Management (ITAM) serves as the foundational basis for organizations to effectively conduct device and endpoint reliability verification. It should function as the starting point for network access control and asset protection policies. Through this, organizations can apply consistent access policies to all devices in accordance with zero-trust principles, thereby significantly enhancing their real-time responsiveness to both internal and external threats.

2. EDR (Endpoint Detection and Response)

Endpoint Detection and Response (EDR) is an advanced security system installed on all endpoint devices within an organization, including PCs, laptops, and servers. It is designed to collect and analyze a wide array of information in real-time, such as running processes, file modifications, user behaviors, and network activities. By doing so, it detects anomalous behaviors and signs of breaches, enabling swift and comprehensive responses. Traditionally, security measures focused on blocking known malware through antivirus solutions. However, EDR has expanded its scope to address unknown threats, insider anomalies, and zero-day attacks, thereby cementing its role as a cornerstone of endpoint security.

EDR (Endpoint Detection and Response) transcends mere threat detection capabilities by conducting real-time correlation analysis of diverse security events occurring within actual work environments. It provides an integrated dashboard that allows for an immediate and comprehensive overview of each endpoint's security status, vulnerabilities, anomalous behaviors, and the execution of unauthorized software, thereby identifying complex threat indicators at a glance. Leading EDR solutions incorporate advanced technologies such as inter-process behavior tracking, memory-based attack detection, file and network forensics, automated vulnerability detection, and user-specific behavior pattern analysis. These capabilities enable security personnel to swiftly recognize abnormal situations and take appropriate remedial actions, either automatically or manually. Furthermore, sophisticated response functionalities, including automated incident response playbooks, automatic isolation of infected endpoints, real-time updates of Indicators of Compromise (IOC), and sandbox integration analysis, are increasingly becoming standardized.

Global Endpoint Detection and Response (EDR) solutions are actively integrating cutting-edge technologies such as artificial intelligence (AI) and machine learning-based detection and analysis, as well as policy automation through natural language prompts. For instance, as illustrated in 'Figure 3' below, when an administrator inputs a prompt in English, such as "Create a detection policy for PowerShell executions containing specific command-line flags," the AI autonomously generates and applies the relevant detection rules. Furthermore, by interfacing with AI-driven threat intelligence, these systems can dynamically incorporate new attack vectors and adversary behavior patterns in real-time, thereby facilitating more intuitive policy adjustments and rule registrations. Alongside these capabilities, a plethora of features are offered to support tailored security operations according to the organization's scale and environment. These include threat hunting functionalities, automated forensics, alert prioritization, behavior-based risk scoring, and optimization of response processes.



Source: CrowdStrike, "Conversations with Charlotte AI Demo"

Figure 3. Interface for Policy Query Generation via Prompt Input

In a Zero Trust architecture, Endpoint Detection and Response (EDR) must function as an indispensable mechanism for verifying the trustworthiness of each device and endpoint. EDR should transcend mere threat detection, enabling the automation of a diverse array of response policies, such as access restrictions, network isolation, and additional authentication requirements, contingent upon the identified risk factors. Furthermore, it is crucial to establish a system that integrates seamlessly with access control systems such as Single Sign-On (SSO), Identity and Access Management (IAM), Multi-Factor Authentication (MFA), and Identity, Credential, and Access Management (ICAM). This integration is essential for the immediate adjustment of access rights for devices or users implicated in a threat, thereby effectively curtailing the propagation of incidents.

Recently, the concept of XDR (eXtended Detection and Response) has emerged, aiming to expand the detection and response capabilities of EDR (Endpoint Detection and Response) to encompass users, networks, systems, and cloud environments. However, the actual implementation of a fully integrated XDR system remains challenging due to limitations such as the scope of data integration, vendor dependency, and the absence of standardized protocols. Consequently, many organizations are opting to establish specialized systems for each pillar, such as EDR, NDR (Network Detection and Response), and SIEM/SOAR (Security Information and Event Management/Security Orchestration, Automation, and Response), and are working towards achieving a pragmatic zero-trust security framework through their interconnection.

Through the implementation of Endpoint Detection and Response (EDR), organizations can transcend mere malware blocking to address a diverse array of threat types and attack vectors in real-time, thereby effectively managing the security integrity of devices and endpoints. Furthermore, leveraging advancements in technology such as AI-driven automation, intuitive policy management, and enhanced interoperability, organizations can equip themselves with the capabilities for real-time security verification and response essential in a zero-trust environment.

3. UEM (Unified Endpoint Management)

Within organizational settings, devices and endpoints were once limited to traditional IT equipment such as PCs and laptops. However, with the evolution of the work environment, there has been a rapid expansion to encompass a diverse array of forms, including smartphones, tablets, wearables, IoT devices, and personally-owned BYOD (Bring Your Own Device). This transformation has significantly increased the complexity of device management, underscoring the necessity for effectively integrating and managing all endpoints through a unified platform.

In response to the evolving environmental landscape, endpoint management technology has similarly progressed, transitioning from Mobile Device Management (MDM) to Enterprise Mobility Management (EMM), and ultimately advancing to Unified Endpoint Management (UEM).

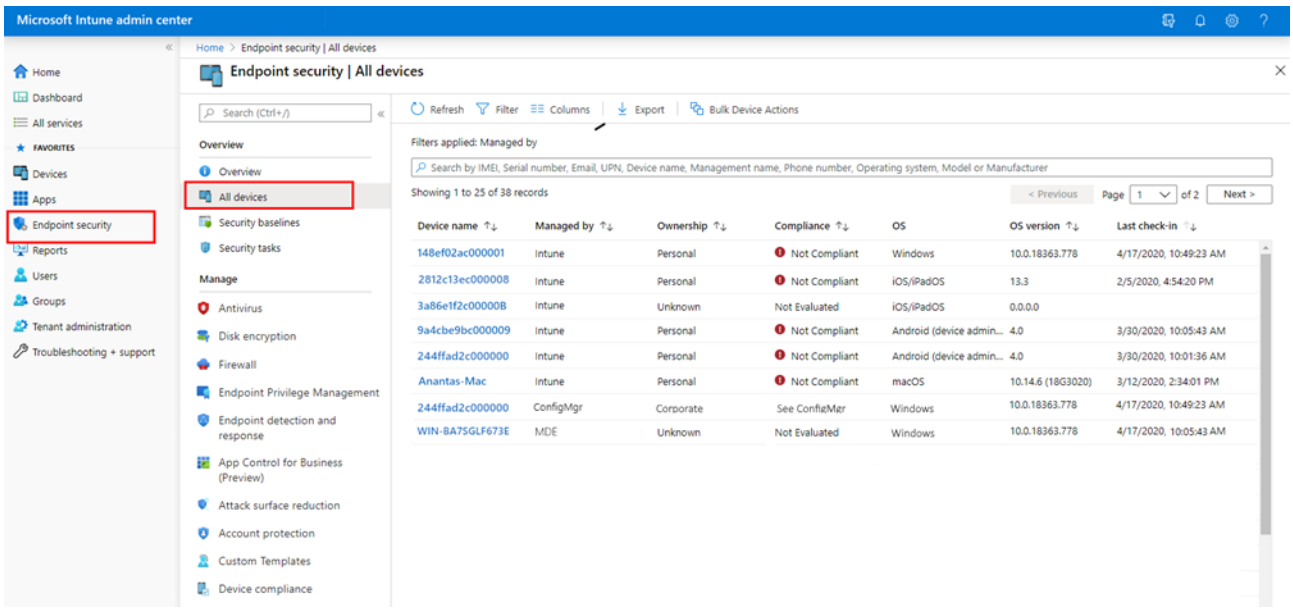
Mobile Device Management (MDM) initially concentrated on remote control and security management functionalities for mobile terminals, such as smartphones and tablets. However, as mobile work environments have progressively expanded and the variety of devices has increased, the limitations of MDM have become apparent.

The concept of Enterprise Mobility Management (EMM) emerged as a solution to overcome these limitations, extending its functionalities beyond Mobile Device Management (MDM) to encompass comprehensive control over the entire mobile environment, including Application Management (MAM), Content Management (MCM), and email and network security. Through the implementation of EMM, the security and flexibility of mobile work environments have been significantly enhanced, facilitating the segregation of work-related and personal applications and data, policy-based access control, and integration with cloud services.

UEM (Unified Endpoint Management) extends the capabilities of EMM (Enterprise Mobility Management) by providing a comprehensive framework for the integrated management of all IT assets and endpoints within an organization, including PCs, laptops, smartphones, tablets, wearables, IoT devices, and BYOD (Bring Your Own Device). This system transcends mere mobile management by unifying the processes of device registration, authentication, policy deployment, security management, application control, vulnerability assessment, data loss prevention, and real-time monitoring across all devices, regardless of operating system, device type, or work environment.
In a zero-trust security architecture, Unified Endpoint Management (UEM) must offer robust control capabilities that verify the status and trustworthiness of all endpoints in real time, and restrict or isolate network access for unauthorized or vulnerable devices. Regardless of whether the devices are for work or personal use, or whether they are owned internally or externally, it is essential to dynamically adjust access permissions and security policies based on the security status, policy compliance, and real-time behavior analysis results of all devices.

Particularly, Unified Endpoint Management (UEM) distinguishes itself by offering comprehensive control over areas that are challenging to manage solely with traditional Endpoint Detection and Response (EDR) systems or IT asset management solutions. For instance, while EDR and asset management solutions deliver high levels of integration, detection, and response capabilities for conventional IT assets such as PCs and servers, they encounter issues like agent compatibility, installation constraints, and control limitations when dealing with mobile devices, tablets, Bring Your Own Device (BYOD) policies, and Internet of Things (IoT) devices, which operate on diverse operating systems and hardware. UEM provides a framework that enables the integrated management of these varied endpoint environments and security challenges within a singular platform. However, there are still relatively few real-world implementation cases both domestically and internationally, and customizing and operating such systems to fit specific organizational environments remains a significant challenge.

To effectively implement a Zero Trust Architecture, it is imperative to actively pursue the adoption and enhancement of integrated endpoint management platforms such as Unified Endpoint Management (UEM). This should be accompanied by concerted efforts to elevate the overall maturity of the endpoint management framework.



Source: Microsoft, "Technical Documentation"

Figure 4. Microsoft Intune, UEM Console Interface

4. AD (Active Directory/PMS, Patch and Asset Management)

Active Directory (AD), a quintessential directory service provided by Microsoft, serves as a pivotal system for the integrated management of various devices such as PCs, laptops, and servers within an organization on a domain basis. Traditionally, it was predominantly utilized for managing user accounts and group permissions. However, in actual corporate environments, it functions as the foundational infrastructure for endpoint management, encompassing device registration, approval, deletion, and policy deployment.

The moment a device is enrolled into the domain via Active Directory (AD), it enables centralized management of a multitude of operational and security procedures. These include the enforcement of security policies on the device, granting of access permissions, deployment of patches and configurations en masse, and aggregation of authentication logs. This centralized management capability extends beyond on-premises AD to hybrid environments integrated with Microsoft Entra ID (formerly Azure AD), thereby facilitating comprehensive device management across PCs, laptops, tablets, and certain IoT devices.

From a Zero Trust perspective, Active Directory (AD) has evolved beyond a mere directory service to function as a comprehensive 'Device Patch and Asset Management System (PMS)' that oversees the entire endpoint lifecycle. For instance, it aggregates and monitors, in real-time, the ownership, location, usage history, and security status—such as patch application and compliance with security policies—of all domain-joined devices. Furthermore, it integrates with Group Policy Objects (GPO) or Intune (Unified Endpoint Management, UEM) to uniformly implement a variety of control frameworks, including automated security configurations, software deployment, anomaly detection, and isolation.

Furthermore, key security solutions such as Unified Endpoint Management (UEM), Endpoint Detection and Response (EDR), Identity, Credential, and Access Management (ICAM), and Zero Trust Network Access (ZTNA), which are integrated with Active Directory (AD), leverage device attribute information and authentication records provided by AD to implement dynamic policies, including network access control, isolation, and additional authentication. This serves as the foundation for practical endpoint security control, enabling the automatic detection and network blocking of unauthorized or unregistered devices, issuing alerts for devices lacking patches, and real-time monitoring of devices accessing critical assets.

Recently, there has been a rapid proliferation of cases where not only on-premises Active Directory (AD) but also cloud-based Entra ID are integrated to manage endpoints within a hybrid environment comprehensively. It appears that various management functions, such as device inventory, patch management, policy deployment, and risk assessment, are progressively evolving towards unification under an AD-based framework.

In a Zero Trust architecture, Active Directory (AD) must function as a comprehensive inventory and policy management engine encompassing both users and devices. The scope of management, data accuracy, and security control capabilities of AD are directly linked to the verification of trustworthiness, access control, and the consistency of policies across all endpoints within an organization. The real-time integrated management provided by various security systems connected to AD serves as a foundation for significantly enhancing the operational efficiency and security posture of the entire organization.

5. EPP (Endpoint Protection Platform)

EPP refers to a suite of products that integratively manage and provide a variety of security functions for endpoints, such as PCs, laptops, and servers, from a single platform. Originally centered around antivirus (AV) and anti-malware solutions, it has recently evolved towards a direction where diverse endpoint security functions, including Endpoint Detection and Response (EDR), Unified Endpoint Management (UEM), Patch Management Systems (PMS), and vulnerability assessments, are converging into a single product suite.

Endpoint Protection Platforms (EPP) typically provide a single console for key security tasks such as real-time endpoint monitoring, policy deployment, threat detection, anomaly analysis, vulnerability assessment, patch management, and software installation tracking. Such an integrated management framework significantly enhances operational convenience and visibility. In the actual market landscape, EPP predominantly manifests as a consolidated solution that integrates various endpoint security measures, such as Antivirus (AV), Endpoint Detection and Response (EDR), and Patch Management Systems (PMS), thereby offering licenses in a unified manner.

However, during the actual implementation phase, the capability of Endpoint Protection Platforms (EPP) to comprehensively integrate and manage all endpoint security systems remains limited. Notably, the majority of EPP products offer integration functionalities that are confined to software from specific vendors, thereby presenting interoperability challenges among security products from different vendors. This limitation fundamentally impedes the seamless integration of diverse security systems required in a zero-trust environment, as well as the centralized and flexible management of threat intelligence, policies, and authentication frameworks across the organization.

Certainly, there are instances where certain organizations integrate APIs provided by endpoint security solutions from various vendors to independently develop their own information security portals or integrated management systems. However, when the term 'EPP' is used in the market, it generally refers to vendor-centric product lines or solutions.

In a zero-trust environment, key security systems such as Endpoint Detection and Response (EDR), Unified Endpoint Management (UEM), Network Detection and Response (NDR), Zero Trust Network Access (ZTNA), Data Security Posture Management (DSPM), and Security Information and Event Management & Security Orchestration, Automation, and Response (SIEM & SOAR) can function as Policy Decision Points (PDP) and Policy Enforcement Points (PEP) within their respective domains. However, if these systems collect and control information solely from their independent perspectives, it may lead to a decline in the consistent application of policies across the organization, real-time risk response, and the integration of security operations.

In a Zero Trust environment, the ultimate objective is to integrate the information provided by security systems across various pillars (PIP) into a top-tier unified platform such as ICAM (Identity, Credential, and Access Management). This integration aims to establish a comprehensive policy and access control framework based on information spanning identifiers, endpoints, networks, and data throughout the organization. ICAM must thoroughly assess identity, authentication, status, risk, and policy inputs from every pillar. Furthermore, it must consistently execute the organization's overarching access policies (PDP) and policy enforcement (PEP) roles from a centralized standpoint.

Ultimately, the independent operation of various domain-specific security platforms, including Endpoint Protection Platforms (EPP), presents inherent limitations in implementing a holistic integrated architecture of Zero Trust. While each system can provide information and participate in policy enforcement, the foundation of a Zero Trust security framework should be the comprehensive control of organizational risks and policies through Identity, Credential, and Access Management (ICAM), which serves as the top-tier integrated management system.

Each system within the device/endpoint pillar must function as a practical mechanism for the technical implementation of a Zero Trust Architecture, transcending mere functional units. IT Asset Management (ITAM), Endpoint Detection and Response (EDR), Unified Endpoint Management (UEM), Active Directory (AD), and Endpoint Protection Platform (EPP) each play crucial roles independently. However, they must also facilitate seamless integration and information sharing to ensure consistent verification of trustworthiness, risk detection, and policy enforcement across all devices within the organization.

The technical implementation and integration of these key systems provide a foundation for establishing consistent security policies and precise controls, even as work environments and device types become increasingly diverse. Within a zero-trust environment, organizations will be able to flexibly respond to the diversification of work settings and device types, thereby substantially enhancing the reliability of endpoint security and operational efficiency.

■ Conclusion

In a Zero Trust Architecture, devices and endpoints transcend their roles as mere operational tools to become fundamental and integral security components that actualize the entirety of an organization's security strategy. Key systems such as IT Asset Management (ITAM), Endpoint Detection and Response (EDR), Unified Endpoint Management (UEM), Active Directory (AD), and Endpoint Protection Platforms (EPP) each perform independent security functions. Simultaneously, they engage in close-knit integration to assess the trustworthiness of all devices, detect real-time threats, and enable comprehensive policy management.

The sophisticated design and operation of device and endpoint pillars ensure comprehensive security management across all organizational devices while providing a 'structural foundation' that allows the organization to adapt flexibly to diverse work environments and the continuously evolving landscape of cyber threats. In particular, the approach of simultaneously verifying and managing both user identity and device reliability serves as a fundamental principle in implementing consistent and robust security controls required in a zero-trust environment.

The Zero Trust-based integrated management framework assists organizations in preventing threats more effectively and responding swiftly, even as the types of devices and usage environments become increasingly diverse and threats grow more sophisticated. This approach transcends the mere effectiveness of individual solutions, contributing significantly to the revolutionary enhancement of an organization's overall security posture and operational efficiency.

In conclusion, device and endpoint pillars constitute a fundamental and indispensable component of a zero-trust architecture, establishing a practical technological foundation for the protection of an organization's digital assets. By continuously advancing technological sophistication and refining management systems centered around this pillar, organizations can effectively reduce the complexity and risks inherent in digital environments to a manageable level, thereby realizing a sustainable digital security landscape.

■ References

[1] NIST SP 800-207, “Zero Trust Architecture”, 2020.08

[2] NIST SP 1800-22, “Mobile Device Security: Bring Your Own Device (BYOD)”, 2023.09

[3] DoD, “Zero Trust Overlays”, 2024.06

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

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

■ References

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

[2] Gartner, “Best Endpoint Protection Platforms Reviews 2025”

[3] Expel, “Expel Quarterly Threat Report, Q1 2025: Endpoint threats”

[4] CrowdStrike, “CrowdStrike Falcon guides”

[5] SentinelOne, " SentinelOne Resource Center, Documentation"

[6] Microsoft, “Microsoft Defender for Endpoint”

EQST INSIGHT

2025.06

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