AhnLab

Case Study

Defending Against BPFDoor Malware with a Next-Generation Security Model

Last April, an incident occurred where the USIM information of many customers of a domestic telecommunications company was leaked due to an external attack. This incident is known to have occurred when a hacker infiltrated the Linux-based server of the telecommunications company and installed BPFDoor-type malware.

Last October, AhnLab utilized its own EDR solution, AhnLab EDR, to detect and publish the analysis results of BPFDoor-type malware similar to the malware used in this attack. The BPFDoor used in the attack has some differences from the malware detected at that time, but its main functions are mostly the same.

In addition to AhnLab EDR, AhnLab leverages the dynamic analysis capabilities of its sandbox solution, AhnLab MDS, to respond to malware, related behaviors, and malicious packets. Detection signatures have also been applied to the Linux server antivirus V3 Net for Linux, the next-generation network security solution AhnLab XTG, the intrusion prevention solution AhnLab AIPS, and the Host IPS of the cloud workload protection platform AhnLab CPP, enabling proactive blocking of BPFDoor. The threat intelligence platform AhnLab TIP promptly shares threat information related to BPFDoor.

Furthermore, AhnLab is presenting a unified solution-and-service security model that covers the entire cybersecurity lifecycle, including ▲prevention and blocking, ▲detection and response, and ▲operations and collaboration, so that its customers can effectively protect their organizations from sophisticated attacks like BPFDoor in the mid to long term.

In this article, we introduce the features of BPFDoor malware, AhnLab's responses, and security measures utilizing AhnLab's next-generation security model.

1. BPF and BPFDoor

BPF (Berkeley Packet Filter) is a mechanism developed for network packet filtering. Installed in the kernel space, it can decide whether to pass packets received from outside to the user space. BPF was first developed around 1992, and in 2014, eBPF (extended BPF) was introduced to the Linux kernel. eBPF supports network packet filtering like the existing BPF but with enhanced performance, security, and stability.

The BPFDoor used in this telecommunications attack is a Linux backdoor that exploits the packet filtering feature of the original BPF. By adding packet filtering rules, it checks if a specific manipulated packet, called a 'magic packet', has been received, and then performs malicious actions. It can bypass server firewalls and security systems, allowing an external attacker to directly send commands to the system, and provides features like reverse shells and bind shells. It can evade security detection and remain hidden in the system for a long time, which provides advantages for carrying out attacks.

BPFDoor malware is open source and was first revealed through a PwC report in 2021. It is known to be used by the China-based APT group Red Menshen (Earth Bluecrow).

2. Features of the BPFDoor Variant That Attacked the Telecom Company

AhnLab detected and analyzed BPFDoor-type malware using AhnLab EDR in October of last year, six months before the telecommunications hacking incident, and published the analysis on the ASEC Blog. The BPFDoor malware detected by AhnLab at that time and the malware used in this telecommunications attack are essentially the same, but there were some differences in specific functions and behaviors.

Analyzed Items	Previous BPFDoor	Variant Used in Telecom Attack (Apr. 2025)
Path for Self-Replication	/dev/shm/kdmtmpflush	Self-replication and deletion functions removed
Disguised Executable Name	udevd, mingetty, etc.	smartd, dbus-daemon, hald-addon-volume, etc.
PID Storage Path	/var/run/haldrund.pid	/var/run/hald-smartd.pid /var/run/system.pid /var/run/hp-health.pid /var/run/hald-addon.pid, etc.
Command Authentication Method	Simple string-based (justforfun)	MD5 (I5*AYbs@LdaWbsO + part of the packet) calculation method

Table 1. Differences between the previous BPFDoor and the variant used in the telecommunications attack

Firstly, the previously detected BPFDoor, as mentioned earlier, self-replicated under the name 'kdmtmpflush' in the /dev/shm path, executed, and then deleted itself. However, the BPFDoor malware identified this time has had this feature removed.

There is also a difference in the PID file path. In the released source code, a PID file is created in the /var/run/haldrund.pid path. This is used to determine whether BPFDoor is running properly. However, the malware used in this attack has a different PID file path.

The command authentication method using passwords has also changed. BPFDoor supports commands such as reverse shell and bind shell, and the commands of the previous malware were distinguished using the password 'justforfun' and the socket string included in each magic packet. However, the BPFDoor used in this attack distinguished commands based on MD5, according to the disclosed indicators of compromise (IoCs). It was a method of distinguishing commands by calculating the MD5 after adding the string received through the magic packet to the string I5*AYbs@LdaWbsO.

The actual functions performed by the malware were mostly the same. However, the content above is based on information released by KISA last April, and as the investigation into the recent telecommunications attack is ongoing, the content may be updated based on the investigation results.

3. How AhnLab Is Responding to BPFDoor

❶ Overview

AhnLab is providing various security measures to enable customers to immediately detect and respond to BPFDoor malware. The role of each solution is as shown in Table 2, and the details will be explained later.

Product Name	Detection Target	Role
AhnLab EDR	All attack-related events	- Detection of activities such as firewall configuration changes and port redirects - Detection of evasion activities targeting security solutions - Understanding attack campaigns through context analysis
V3 Net for Linux Server	Known malware	- Signature-based detection and remediation of malware infiltrating the server
AhnLab XTG	Known malicious packets	- Signature-based blocking of 'magic packets' (firewall's IPS feature)
AhnLab AIPS	Known malicious packets	- Signature-based blocking of 'magic packets'
AhnLab TIP	All attack-related threat information	- Apply the latest malware trends and IoC information to security operations
AhnLab MDS	Known malware and malicious packet attack-related events	- Signature-based detection and remediation of infiltrating malware - Signature-based blocking of 'magic packets' - Detection of firewall configuration changes, port redirects, security solution evasion activities, etc. (dynamic analysis)
AhnLab CPP (Host IPS)	Known malicious packets	- Signature-based blocking of 'magic packets'

Table 2. AhnLab solutions' response details to BPFDoor malware

❷ BPFDoor Detected by AhnLab EDR in October 2024

According to last year's BPFDoor detection details by AhnLab EDR, one of its characteristics is that it copies itself to the /dev/shm path under the name kdmtmpflush during execution. AhnLab EDR detected the behavior of a suspicious process self-copying to the /dev/shm path and granting execution permissions as a threat, as shown in Figure 1. This enabled the security manager to recognize threats in advance.

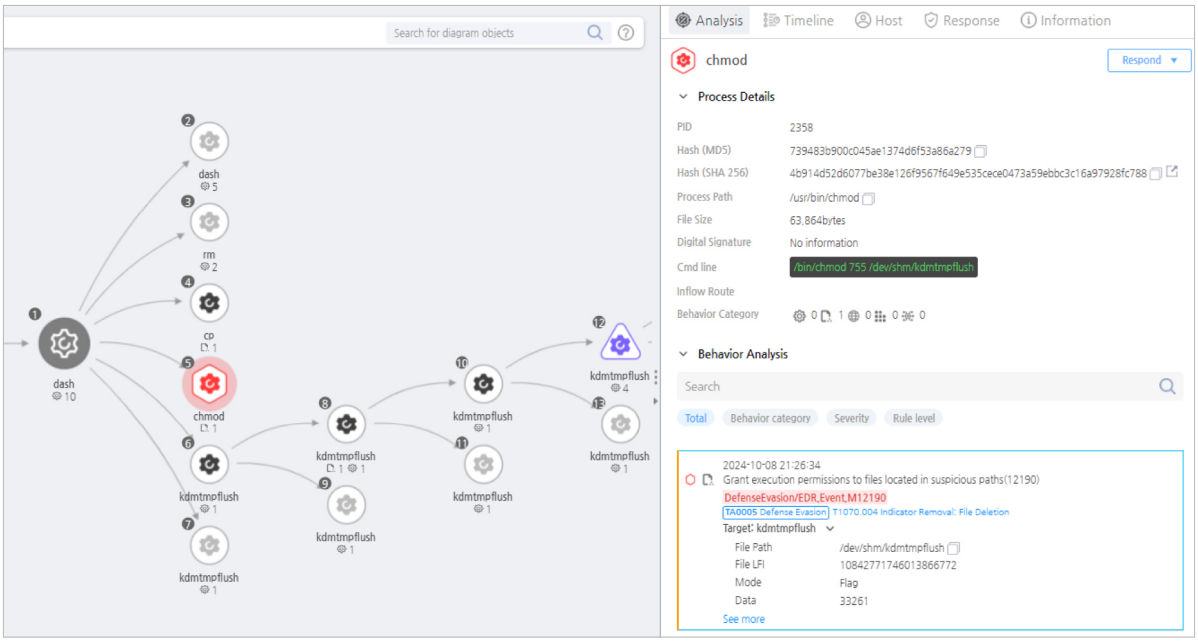

Figure 1: Detection of the behavior of granting execution permissions to a file located in a suspicious path

Additionally, when a command containing a password matching the 'magic packet' is received, it opens a specific port, changes the firewall settings, and redirects packets received from the attacker. AhnLab EDR detected the act of adding and removing new rules using Iptables and activities like port redirection as suspicious behaviors.

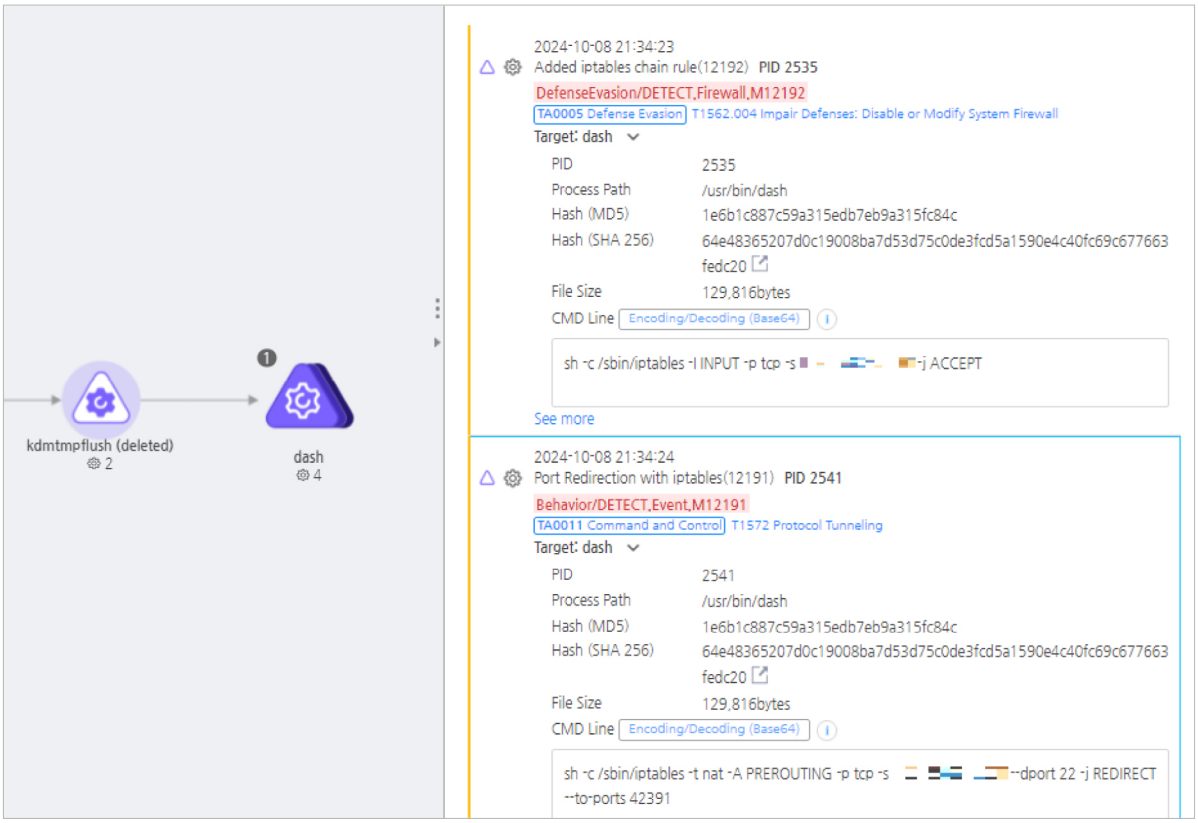

Figure 2. Detection of rule addition and port redirection activities using iptables

These actions are techniques also found in other malware, making it difficult to conclude that it is BPFDoor malware based on this alone. AhnLab EDR additionally analyzed and synthesized suspicious activities of malware, such as C2 communication, and detected it as BPFDoor, as shown in Figure 3.

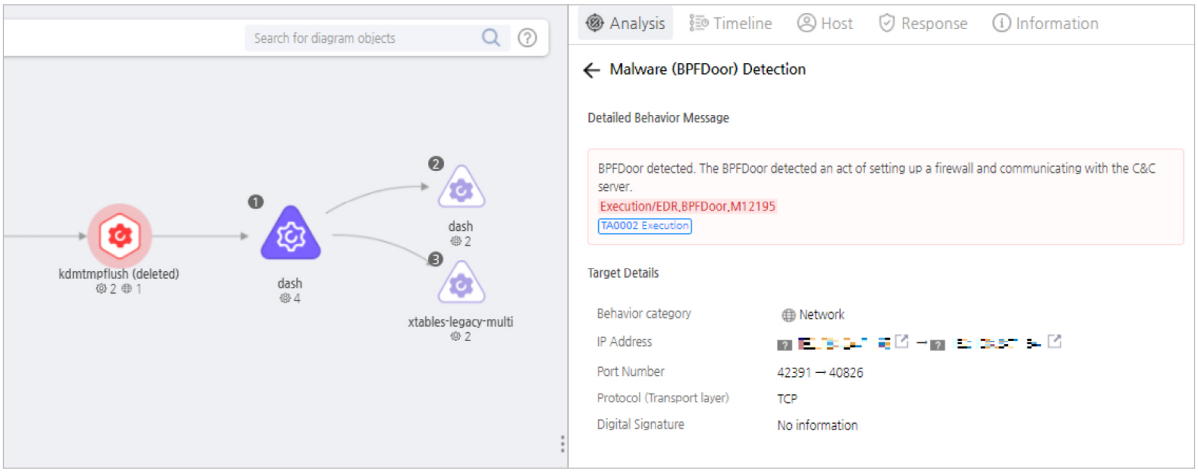

Figure 3. BPFDoor malware detected by AhnLab EDR

From the customer's perspective, they could identify the cause and take appropriate action by utilizing AhnLab EDR to check the analysis information and context related to suspicious activities of BPFDoor.

AhnLab EDR, which effectively detected advanced malware and attack techniques like BPFDoor, has uniquely participated four consecutive times in the globally recognized security product test, the 'MITRE ATT&CK Evaluation,' as a Korean security company, proving its excellence. The MITRE ATT&CK Evaluation assesses the threat detection and response capabilities of participating products based on scenarios simulating the attack techniques of major threat groups.

In particular, in the recently conducted Round 6, AhnLab EDR detected 95% of the scenarios composed of actual attack techniques carried out by the major ransomware groups CL0P and LockBit across Windows and Linux. This is a top-tier performance among global security companies. Moreover, it received the highest rating of 'Technique' in 49 out of 56 detected substeps, which is evidence that users can comprehensively understand the 'context' of threat activities through detection information.

Detailed information about AhnLab's MITRE ATT&CK Evaluation Round 6 results can be found in the Results Analysis Report.

❸ Immediate Response With Signatures and Threat Intelligence

AhnLab not only provides detection and analysis through AhnLab EDR but also leverages the dynamic analysis capabilities of its sandbox solution, AhnLab MDS, to respond to malware, related behaviors, and malicious packets. It applies detection signatures to its Linux server security solution, V3 Net for Linux Server, to help customers detect and block BPFDoor-related attacks in advance. User-defined signatures are also added to the next-generation firewall AhnLab XTG, the intrusion prevention solution AhnLab AIPS, and the Host IPS of the cloud workload protection platform AhnLab CPP, enabling malicious packet inflow to be blocked at the network level. In this way, AhnLab incorporates publicly available information, such as IoCs, into its solutions in real time to protect customers from potential threats posed by BPFDoor.

Furthermore, the threat intelligence platform AhnLab TIP provides comprehensive security information, including BPFDoor-related IoCs and the latest trends, to support customers in efficiently protecting their organizations.

4. Secure Your Organization's Future With a Next-Generation Security Model

This BPFDoor attack goes beyond simply exploiting vulnerabilities; it bypasses security solutions to infiltrate internally and conducts attacks over a long period, representing a case where sophisticated techniques have been realized. Although it is important to respond to the immediate cases of damage caused by BPFDoor, a strategy is needed to effectively address various threats from a long-term perspective. In response to this, AhnLab presents a unified solution-and-service security model that encompasses the cybersecurity lifecycle, including ▲prevention and blocking, ▲detection and response, and ▲operations and collaboration.

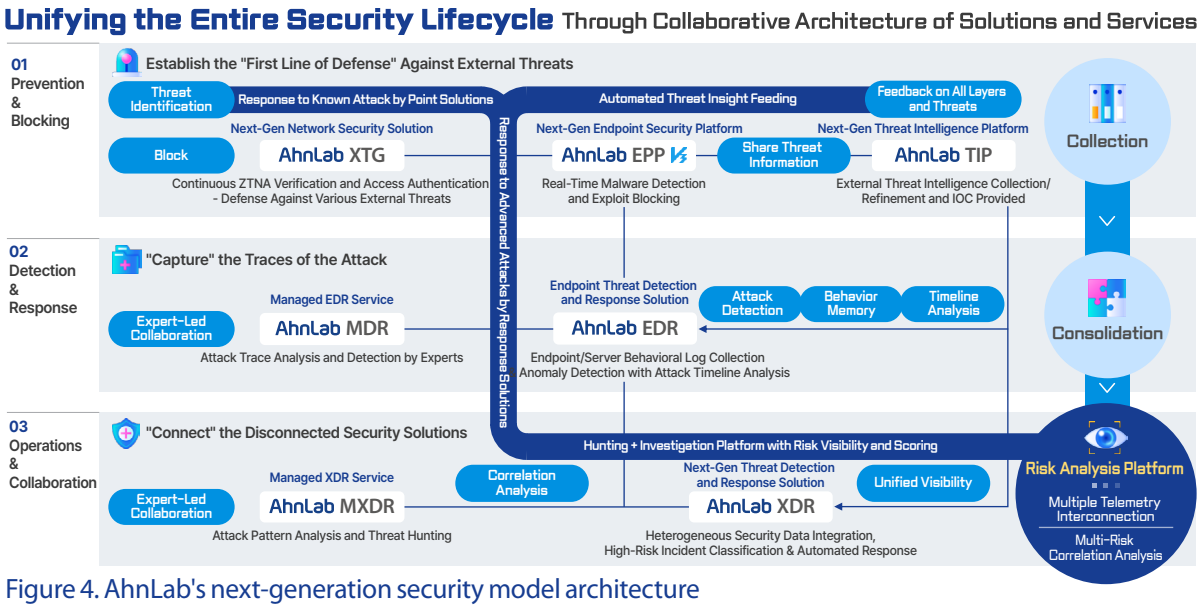

Figure 4. AhnLab's next-generation security model architecture

❶ Prevention and Blocking

In a next-generation security model, the most important task is to establish a system that can prevent and block threats in advance. At this stage, by integrating and utilizing AhnLab's new next-generation firewall, AhnLab XTG, the endpoint security platform, AhnLab EPP, and the threat intelligence platform, AhnLab TIP, significant results can be achieved.

A. AhnLab XTG: Threat Blocking and Continuous Verification of Network Access

The next-generation firewall, AhnLab XTG, is an advancement from the existing AhnLab TrusGuard and blocks threats at the forefront of the network based on enhanced performance. Especially, the Zero Trust Network Access (ZTNA) feature of AhnLab XTG continuously monitors the identity and security status of users and devices to ensure that only verified users can access applications and network resources. By doing so, it is possible to preemptively block server access by unauthorized users and devices, minimizing potential damage.

B. AhnLab EPP (V3 Net for Linux Server): Malware Blocking and Unified Management

Recently, as Linux server vulnerabilities and malware increase, the need for security is also rising. By using the long-validated Linux server antivirus V3 Net for Linux Server, you can preemptively detect and block sophisticated new and variant malware like BPFDoor. By using AhnLab EPP as well, you can integrate and manage detection status, policies, events, etc., enabling quicker response. Additionally, in addition to antivirus, you can further enhance endpoint security by utilizing the advanced rules among various security functions provided by EPP, such as patch management, security status checks, and device control.

C. AhnLab TIP: Intelligence-Based Strategy Development and Internal Impact Assessment

AhnLab TIP provides various threat intelligence, including the latest indicators of compromise (IoCs), analysis reports, and threat group analysis, regarding cyber threats. Especially, based on data collected through AhnLab's various solutions, it can analyze and categorize threats, providing customers with unique threat intelligence that cannot be found in other companies. From the customer's perspective, the latest IoCs identified in AhnLab TIP can be automatically applied to AhnLab XTG and EPP, and by performing an assessment of the internal impact, they can establish a threat prevention system.

❷ Detection and Response

Latest malware, such as BPFDoor, often comes equipped with capabilities to evade security solutions. If a cyber attack bypasses and infiltrates the first-line defense system, a more comprehensive concept of detection and response is needed. By utilizing AhnLab EDR and MDR services, you can respond to threats based on broad visibility.

A. AhnLab EDR: Verified Threat Detection and Response Capabilities

As previously introduced, AhnLab EDR has detected and analyzed activities related to BPFDoor in detail. By monitoring and logging all activities occurring at the endpoint and analyzing their relationships and context, it supports the correct understanding and response to any threat. Such excellent context analysis capabilities not only minimize damage caused by incoming attacks but also greatly assist in establishing a recurrence prevention system in the future.

B. MDR Service: Powerful Detection and Response With Experts

EDR, which requires expertise in operation, may not be easy to manage for small businesses. AhnLab's MDR service, supported by top industry experts, enhances detection, analysis, and customized response, reducing the operational burden on customers while elevating detection and response capabilities to a new level.

❸ Operation and Collaboration

Latest cyber threats target an organization's assets by crossing various domains such as endpoints, networks, clouds, and emails. If responding to these threats based on point solutions, visibility is lowered, and there are also limitations in terms of management. Therefore, the need for a platform that can comprehensively manage risks across the entire organization, combined with professional services, is emerging.

A. AhnLab XDR: Systematic Risk Management Based on Integration

The integrated risk management platform AhnLab XDR analyzes and normalizes data collected from various areas to quantify risks and visualize the relationships of cyber attacks. In addition, it aims for Open XDR, flexibly integrating with various security solutions to present optimal response measures. Equipped with AI technology that supports XDR's detection, analysis, and response, it enables even more convenient risk management.

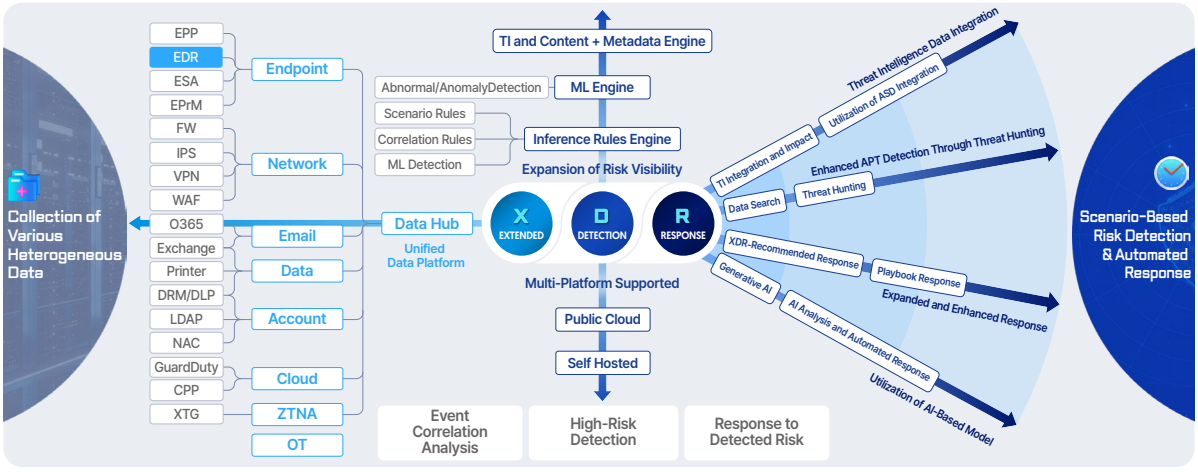

Figure 5. AhnLab XDR-based risk management concept diagram

B. MXDR Service: High-Quality Detection & Response and Threat Hunting

Operating an XDR platform that covers all security areas also requires expertise above a certain level. The MXDR service, which supports customers' XDR operations, involves our experts continuously monitoring XDR events and analyzing detected risks in detail. In addition, by assessing the internal impact of risks and responding to them, while also supporting proactive threat hunting, it enables more proactive prevention of breaches.

5. Conclusion: A Time When the Synergy of the Best Platform and Experts Is Needed

Recent global trends show a tendency to emphasize the value of "cooperation". This means that in responding to increasingly sophisticated cyber threats, not only are top-level solutions important, but collaboration between people is also crucial. Since no security solution can be perfect, these limitations must be addressed through a flexible, integration-based security approach combined with human expertise.

AhnLab plans to continue leading by combining the synergy of security platforms and experts, based on the next-generation security model introduced in this document, to enable customers to build a seamless security system.

AhnLab

AhnLab, Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, South Korea
www.ahnlab.com / global.sales@ahnlab.com