AhnLab

Case Study

Driving Security Innovation for Semiconductor Company with AhnLab EDR and MDR

Company S is a PMIC (Power Management Integrated Circuit) solution specialist and is comprised of top power semiconductor experts. The company has a top-tier lineup of analog and power semiconductor products in Asia and supplies them in large quantities to major smartphone, TV, laptop, and PC manufacturers both in Korea and internationally.

Introduction

In September 2023, the Korean PMIC (Power Management Integrated Circuit) company S implemented AhnLab EDR for the first time. The company had been maintaining security with AhnLab's V3 products (V3 Internet Security, V3 Net for Windows), but after reviewing new options for effective defense against incidents and enhanced security, they decided to adopt AhnLab EDR. AhnLab EDR is provided along with MDR service, offering real-time threat detection and monitoring, as well as transmitting detected event logs to AhnLab's remote SOC platform. Through this, AhnLab's security experts analyze and respond to threats, establishing a comprehensive security system. Additionally, AhnLab provides Company S with regular threat analysis and monthly statistical reports to prepare for additional threats.

By adopting AhnLab EDR, Company S is building a more robust security infrastructure and significantly enhancing operational efficiency and stability. In addition to AhnLab EDR, the company also operates AhnLab EPM (EPP Patch Management) for patch management and AhnLab EPP Management, which allows for integrated management of EDR, EPM, and V3.

Benefits

· Establishment of a real-time monitoring system for client PC activities
· Early detection and proactive response to signs of hacker intrusion
· Enhanced security visibility through regular threat reports

· Improving operational efficiency through unified management with a single agent
· Enhancing user convenience with intuitive and simple security management without complex configurations

· Minimizing data loss and achieving system restoration with automatic data recovery in the event of a ransomware incident
· Maintaining service continuity through automatic response and system recovery when a threat occurs

Impact of AhnLab EDR on Organizations

Quantitative Benefits

- Enhanced security incident detection rate
- Decreased security threat response time
- Reduced security operation costs

Qualitative Benefits

- Simplification of threat response system
- Improved transparency of security posture within the organization
- Support of rapid decision-making
- Enhanced business productivity

> Since adopting AhnLab EDR and MDR, we have seen significant benefits in threat detection, response, and operational management. With real-time threat detection and an automatic response system, the anomaly detection rate has improved, enabling more efficient prediction and prevention of potential breach incidents. Additionally, thanks to automated responses and remote support from AhnLab security experts, the workload of security personnel has been significantly reduced. In particular, we evaluate AhnLab EDR as a highly suitable solution for our business environment due to its excellent PC behavior analysis feature, which was what we needed the most.
>
> - Security Technology Manager, IT Team, Company S

Customer Story

How are AhnLab EDR and MDR affecting your current business environment?

Since adopting AhnLab EDR and MDR, we have experienced tangible improvements in our security posture. Thanks to real-time threat detection and an automated response system, the speed of response to security incidents and the efficiency of security management have greatly improved. Additionally, the MDR service provided with EDR is convenient because it offers not only threat detection and monitoring but also analysis results and solutions for detected threat events. AhnLab EDR goes beyond simple alerts by providing specific response measures, significantly reducing the workload of security personnel. It allows for quick identification of causes and a clear understanding of response methods when anomalies occur, enabling proactive defense.

Quantitative Benefits: The detection rate of system anomalies and security incidents has significantly increased, enabling the proactive prevention of potential threats that were previously undetected. In addition, the incident response time has been reduced, and security operation costs have been significantly decreased.

Qualitative Benefits: With the simplification of the threat defense process through automated detection and response, operational efficiency and business productivity have increased, and the stress on security personnel has been reduced. Additionally, MDR analysis reports have provided management with transparent visibility into the security posture, greatly aiding in quick decision-making regarding security issues. As a result, not only has the incident response speed improved, but overall business productivity has also increased.

What were the reasons for selecting AhnLab's EDR among various companies?

While reviewing measures to effectively defend against breaches and enhance security, the decision was made to adopt EDR. After conducting a PoC for about a month and comparing another security company B with AhnLab, we ultimately selected AhnLab. AhnLab built trust by demonstrating a proactive attitude and quick response in understanding customer needs. Above all, what I was most impressed about AhnLab EDR was its user-friendly and convenient UI, as it integrates seamlessly with the existing V3 product line. In addition, AhnLab's products have excellent compatibility with other third-party security solutions. The superior management efficiency it provides through seamless integration with existing in-house solutions was the key differentiator. We expect to achieve successful outcomes through continued collaboration with AhnLab in the future.

Key Strengths of AhnLab EDR Recommended by Customers

- Real-time threat detection, automated response, and monitoring
- Simplified management and high compatibility through a single agent
- Regular threat analysis reports Ransomware recovery and data protection
- Professional technical support

What aspects of AhnLab EDR do you find more suitable compared to Company B's product?

Company B proposed a product from Company T, a global vendor. This product offered extensive features and a variety of customizable settings. However, the UI was complex and not intuitive, making it somewhat difficult to fully understand all features and utilize them according to specific requirements. Additionally, despite offering various features, there were aspects that did not align with our business environment in practical use, and there were shortcomings in the responsiveness of the representative. On the other hand, AhnLab EDR proved to be a more suitable choice for us, offering a user-friendly UI and features optimized for our requirements.

What are the most important principles or criteria your company considers when selecting IT and security products?

First, we prefer products with proven track records and extensive references. Along with this, we review whether the product aligns well with the organization's characteristics and operating environment to minimize system crashes and management difficulties, and we carefully consider compatibility with existing solutions.

Considering these criteria comprehensively, we believe AhnLab's security solutions are a trusted partner that can provide excellent security features, technical support, and operational stability tailored to our organization's IT environment, based on their established reputation and proven track record of customer trust.

What are three key advantages you have experienced while using AhnLab EDR?

1) AhnLab EDR is a lightweight solution, and all management can be handled with a single agent on AhnLab EPP. This enables efficient security management without requiring additional management tools or complex configurations, minimizing the impact on the organization's IT infrastructure. Additionally, unified management through a single agent increases operational efficiency and reduces management costs.

2) Using AhnLab EDR, you can monitor in real-time where and what actions occur, and preemptively block malicious activities. For example, when PowerShell is executed, it can distinguish whether the entered command line is a legitimate PowerShell command or a malicious one.

3) AhnLab EDR provides an automatic rollback feature that quickly restores data to its previous state if important files or systems are encrypted or damaged during ransomware or other cyber attacks. This enables system users to reduce data recovery time and minimize data loss. As a result, it has alleviated psychological anxiety about ransomware attacks that could cause significant damage to the organization and has instilled confidence in the ability to quickly return to normalcy even if a security incident occurs.

Synergy Between AhnLab EDR and MDR

· Immediate threat recognition and remote response from experts
· In-depth threat analysis and customized response strategies
· Improvement of security operations and management efficiency

What is the level of satisfaction with the service and technical support after implementing AhnLab EDR?

Overall satisfaction with AhnLab's technical support is very high. The most positive aspect is the quick response to support tickets. While it varies with the complexity of the analysis subject, generally, a response for problem resolution is received within a day of submitting a ticket, enabling rapid response even in urgent situations.
The monthly MDR analysis reports are also being used effectively. These reports provide customized security analysis and threat detection information for the organizational environment, which greatly helps in accurately assessing the current situation and determining subsequent response measures. We have not found any areas for improvement in the report's content and are fully satisfied with the current level of service.

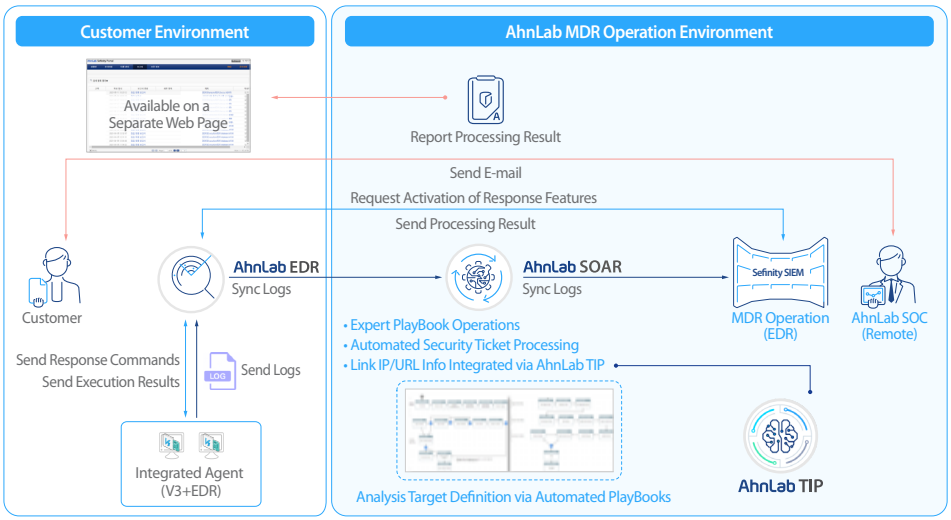

Figure 1: MDR System Configuration

Conclusion

In conclusion, AhnLab EDR and MDR play a crucial role in enhancing the organization's security level. These solutions provide an environment where security personnel can resolve issues quickly and proactively respond to threats through real-time threat detection, monitoring, automatic response, and recovery systems.
In particular, the combination of AhnLab EDR and MDR contributes to enhancing the quality of security management by providing in-depth analysis and specific solutions for security incidents, beyond simple threat detection. Furthermore, providing analysis results and response plans for security threats to management supports quick decision-making and significantly improves business productivity.
AhnLab EDR maximizes the efficiency of security operations through excellent compatibility with existing solutions, an intuitive and user-friendly interface, and easy management. Moreover, AhnLab's fast and professional technical support is highly rated by customers, and regular MDR reports are crucial for accurately assessing security posture and developing effective response strategies.
Overall, AhnLab EDR demonstrates excellent performance not only in strengthening organizational security but also in terms of operational and management efficiency. Moving forward, AhnLab will continue to establish itself as a reliable partner in enhancing customers' security capabilities through ongoing collaboration with various industries.

AhnLab

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