2018. 08. 22

A Simple Guide to Understanding EDR

Proposition for Adopting Next-generation Endpoint Security Technology

AhnLab

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, South Korea

Tel: +82-31-722-8000 | Fax: +82-31-722-8901 | www.ahnlab.com

Table of Contents

Overview

In the age of growing cybersecurity threats, security vendors and customers are focusing on endpoint detection and response (EDR) solutions as their key security solution.

The rapid growth of interest in the EDR market is fueled by a need for threat visibility and increased responses that supplement the limitations of existing solutions. Will EDR represent the new generation for security solutions? Or will it be another flash in the pan?

This report covers the background that has led to the need for EDR, the demands of the market, and a brief description of the recently released AhnLab EDR.

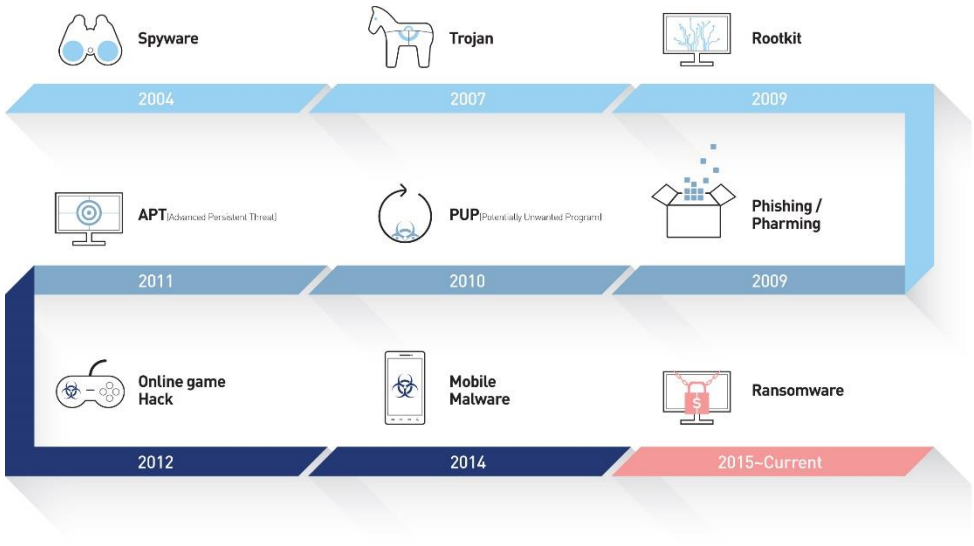
How EDR Was First Introduced

01. Changes in Security Threat Trends

In 2017, massive cyber incidents were reported around the world. A number of corporations, such as Equifax, Uber, and Verizon, suffered data breaches that exposed the personal information of their users. Moreover, ransomware such as WannaCry and Petya created chaos worldwide; this includes the infamous Erebus ransomware, which led to the bankruptcy of a large Korean web hosting company.

All these attacks used endpoints as their first point of entry and were propagated through malware. This attack pattern has been used for the last 30 years since the release of Brain, the first computer virus, in 1986.

One difference today is that malware technology has evolved to elude detection by security solutions. The past examples show us that attackers will continue to use malware and adjust to override the successful efforts of defenders. There is a need for an effective strategy and solution that can provide integrated management and response to endpoint threats.



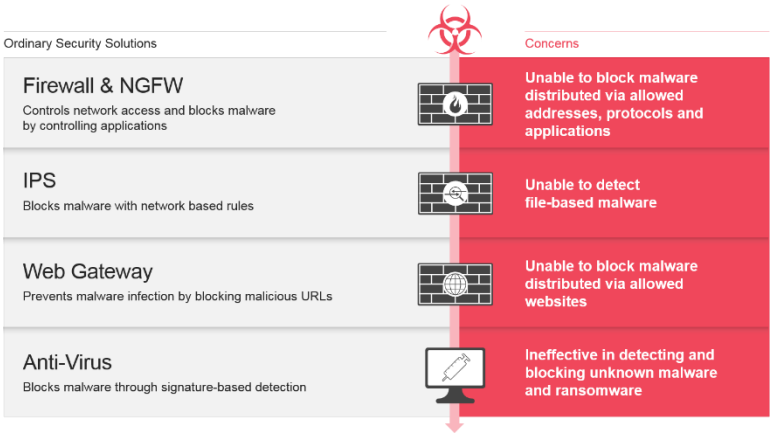
[Figure 1] Overview of Main Changes in Cyber Security Threat Trends

02. Limitations of Existing Security Solutions and Market Demands

A change in threat response strategies is required not only for the security industry, but also for customers using security solutions, such as corporations and public institutions. Most corporations, in general, have been using anti-virus (AV) products, patch management, media control, and network access control for endpoints; for networks, they have been using firewalls, intrusion prevention systems (IPS), DDoS defense systems, and web application firewalls (WAF). However these security measures have not been able to prevent losses for many corporations due to malware infection, traffic overload, and data leakage.

Attackers are using increasingly sophisticated methods of attack that are difficult to detect by traditional means and that even elude detection by advanced persistent threat (APT) solutions. Unpatched applications and vulnerable websites are easy targets and one of the more common methods of infection. Moreover, network security products have limitations in blocking malware intrusion with their method of permitting access from authorized addresses, protocols, and applications.

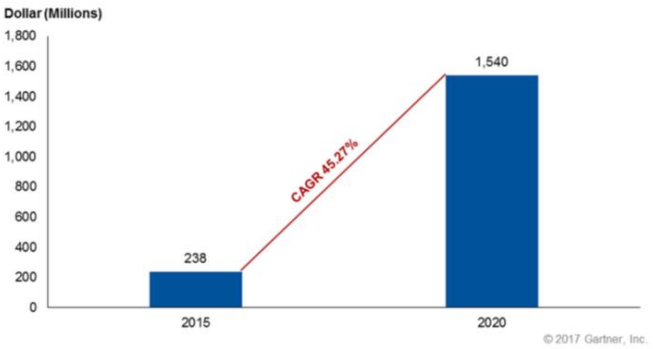
User and entity behavior analytics (UEBA) solutions and security information and event management (SIEM) solutions that are based on relatively new technologies also do not guarantee 100 percent protection. UEBA is behavior-based so it requires a separate data collection server to collect and store information like SIEM. SIEM is rule-based but is dependent on the linked security product as it cannot analyze the logs if they are not delivered by the linked product.



[Figure 2] Limitations of Existing Security Solutions

Corporations are beginning to understand that traditional security solutions are not equipped for today's threat landscape. They understand the need to prepare against unknown threats such as new malware or zero-day exploits, and the need to respond against invisible threats that can happen at any time and in any form. There is also a need for a solution to quickly detect and respond to these types of threats before irrevocable damage has occurred.

This is where an EDR solution comes into play. The demand and interest for EDR is blooming not only in South Korea but all over the world. According to the global research firm, Gartner, the global EDR market will grow at a compound annual growth rate (CAGR) of 45.27 percent from $238 million in 2015 to $1.5 billion in 2020. In addition, it is expected that by 2020, more than 65 percent of large corporations and over 50 percent of small and medium-sized companies will invest in a full-featured EDR.



[Figure 3] Endpoint Detection and Response Market Revenue (*Source: Gartner)

Definition of EDR

Then what exactly is EDR? The term "EDR" was first coined in 2013 where it was originally listed as "ETDR," or “Endpoint Threat Detection and Response,” in the Gartner blog. Since then, Gartner has published an annual report titled *Market Guide for EDR Solutions*, which gives information on the EDR market, technology trends, and key vendor news and developments.

Gartner defines EDR as a security solution that provides continuous monitoring and response at the endpoint level. It states that an EDR solution has four features: detects security incidents; investigates security incidents; contains incidents at the endpoint; and remediates endpoints to their pre-infection state.

In other words, EDR must quickly and effectively detect and analyze diverse behaviors occurring at endpoints and must provide visibility to track violation behavior, such as identifying which device was affected. Once an infected device is detected, it must also isolate the infected device or block the network and provide an appropriate response, such as patching the vulnerability. The purpose of all these actions is to minimize the dwell time and damage of the threat.

Most security vendors around the world now offer EDR solutions. Vendors that provide endpoint protection platforms (EPP) such as AhnLab, Symantec, and Trend Micro, are releasing or preparing products for the market by adding EDR modules to their existing products. Next-generation anti-virus vendors and new EDR vendors are also releasing products to gain a share of the market.

Endpoint Platform-based AhnLab EDR

AhnLab recently released AhnLab EDR together with the next-generation endpoint security platform, AhnLab EPP.

As endpoint security lies at the center of the security industry's key interests, some touted AhnLab's release as "the return of the king." However, AhnLab has continuously emphasized the importance of endpoints since it was founded in 1995. In 2017, AhnLab released its endpoint security platform strategy, AhnLab SECURITY, to highlight the need for innovation in endpoint security.

AhnLab Security LADDERS stands for Legacy, Adaptive, Detection, Driven, Endpoint, Response, and Service, and expresses customer-driven, easy-to-implement security.
► See More on AhnLab Endpoint Security Platform Strategy <Security LADDERS>

AhnLab has used this strategy to focus on the role of threat management and incident response from malware detection and has built a Detection-Analysis-Response system for rapid detection and response as well as defense via blocking.

An EDR solution needs to efficiently collect, store, and analyze vast amounts of data while linking with various security solutions at the same time. Therefore, it requires a new platform equipped with the necessary architecture. AhnLab EPP is this next-generation endpoint protection platform – and this is the reason that AhnLab has released AhnLab EDR along with AhnLab EPP.

A typical endpoint protection platform, which is an endpoint security solution for file-based malware protection, provides detection and prevention of malicious activity in applications and conducts investigation and remediation to respond to security incidents.

AhnLab EPP is a next-generation platform that detects, monitors, and responds to ongoing security threats through organic integration and linkage to various AhnLab endpoint security solutions. The main advantage of AhnLab EPP is that it is a single agent, single management console that provides organically integrated management of multiple solutions.

[Figure 4] AhnLab EDR on AhnLab EPP Interoperating With Other Security Solutions

For example, customers using AhnLab V3 and AhnLab EPP agents only need to add the license without any agent installation to use AhnLab EPP for integrated management, monitoring, and response. Also, customers can use the management console to select products suitable for their needs, such as AhnLab Patch Management for OS and security patch management; AhnLab ESA for detecting and remediation of vulnerable systems; and AhnLab Privacy Management for blocking files suspected of leaking personal information.

Conclusion: Proposition for Adopting Next-generation Endpoint Security Technology

The EDR market is converging with the EPP market at a fast pace and EDR, EPP, and other next-generation endpoint security products will be redesigned into a single agent, single management console method within the next three to five years. Existing EPP companies are quickly adopting EDR functionalities to better monitor attackers, and EDR vendors are adding better detection and response capabilities to compete with and replace other EPP vendors.

As many security vendors are releasing EDR products due to the rising demand, EDR is being recognized as the key to many security problems. There is no doubt about the critical role that EDR will play in security, but we must not forget that EDR is just one more tool we can use to respond to security threats. We should keep in mind that EDR must be accompanied by administrator's cooperation and implementation processes to see its potential fully utilized.

