"Dramatically reduced the cost of endpoint security measures"

ALL NIPPON AIRWAYS CO., LTD.

Industry	Aviation service industry
Scale	1,974.216 billion yen in sales (ANA Group as a whole; fiscal year ending March 2020)

Established in 1952 and headquartered in Minato-Ku, Tokyo, All Nippon Airways is the core airline business of the ANA Group and has the largest route network in Japan for both domestic and international flights. Based on the Group's management philosophy of "Built on a foundation of security and trust, "the wings within ourselves" help to fulfill the hopes and dreams of an interconnected world." ANA operates domestic flights to 47 airports nationwide. As a member of the Star Alliance, the airline flies to major cities in Asia, North America, and Europe, and will carry 42,916,000 domestic passengers and 9,416,000 international passengers in the fiscal year ending March 2020.

Challenges

1. There was a concern that neither pattern matching, behavior detection, nor EDR could completely stop the attack.

2. The cost of securing and training personnel to respond to increasingly sophisticated cyber-attacks has become prohibitive.

Effects of the introduction

1. As it becomes more and more difficult to find and deal with the huge number of new viruses that occur every day, the introduction of AppGuard, which thoroughly protects the OS and prevents harmful actions against the OS, will eliminate threats to endpoints and allow us to operate our infrastructure with peace of mind.

2. Fundamentally different from anti-virus software, AppGuard protects the normal operation of systems that are developed according to the Windows development standard process. Therefore, once the policy is set, there is no need to test it before company-wide deployment, even if the product is upgraded. Thereby, costs can be kept to a minimum and endpoints can be protected from threats even without advanced security knowledge and expertise.

Background of the introduction

In order to protect 25,000 terminals, we had installed security software in the following order: pattern matching type, behavior detection type, and EDR. The pattern-matching type had a low virus detection rate, and we had to send people to update virus definition files for sites with narrow bandwidth, which was costly. The behavior detection type that was introduced after that needed to be upgraded as attacks became more sophisticated and new behaviors were discovered. Each time a version was upgraded, it had to be tested and deployed in each system, which was very expensive. The EDR was introduced on the assumption that there would be an intrusion. Still, we had to shorten the response time, so we had to set up a new 24/7 monitoring system, and our staff had to have advanced knowledge of shift work, procedures, and viruses, as well as the know-how to respond. However, there is a limit to the number of highly skilled security personnel acquired and trained. Therefore, we decided to introduce AppGuard because it would eliminate testing and deployment costs and the need to train highly trained security personnel.

Key points of selection

1. We evaluated the completely new security concept of "not letting what should not be done" instead of judging whether it is a virus or not.

2. Even if the version is upgraded, the core technology remains the same and there is no need for extensive testing. The monitoring system for detection and response could also be reduced, and we came to the conclusion that the cost effectiveness was excellent.

Dramatic reduction of security measure costs is now possible

Conventional security software was designed to determine whether a program was a virus or not. On the other hand, AppGuard was a completely new way of thinking: 'Don't let the OS do anything it shouldn't do. I thought it was very innovative, but I had my doubts about whether it would really protect the devices, so we conducted a test implementation in our department along with a research. As a result, we were able to demonstrate its protective power by ensuring the safety of the OS and protecting the normal operation of the system. After the introduction of the system, it was determined that testing for company-wide deployment would no longer be necessary and costs could be dramatically reduced. We concluded that the cost-effectiveness of the system was very good, and we started to implement it in 2018. And in March 2019, we completed the deployment to all 25,000 terminals in the company.

AppGuard is the only way to prevent intrusion and is standard across the company

When we deployed AppGuard, we tested it to make sure it worked as theoretically intended. As a result, applications that were developed according to the standard Windows development process were launched without any problems and did not require any additional configuration. On the other hand, systems that did not follow the standard development process were stopped, but this could be solved by tuning the policy. Unlike whitelist-type products, detailed operations are not required and policy configuration is not very difficult. Once you operate AppGuard and get used to it, it becomes easy.

However, it was necessary to change the mindset of the IT department, which was used to the old security software, and there was a lot of resistance, especially in the department in charge of deploying the software to the field. However, there was a case of an external intrusion attempt at the end of 2019, and AppGuard was the only one among multiple detection systems, including multi-layered protection, that prevented it. This event has completely changed the mindset of the IT department. Now, AppGuard is a standard feature on all company-issued PCs.

Future Prospects

The Coronavirus disaster has changed the way employees work, and more and more employees are teleworking. Until now, most of the terminals taken outside the office were VDI, but depending on the type of work, PC performance may be insufficient. Therefore, we will gradually switch to fat PCs with AppGuard installed. We are also considering deploying AppGuard to all ANA Group companies as part of our efforts to strengthen the supply chain.

Akihiro Wada, All Nippon Airways Co., Ltd., Digital Transformation Office, General Manager, Planning & Promotion Department, Information Security and Infrastructure Strategy

Blue Planet-works
Safety for the Connected World

Blue Planet-works, Inc.
Daiwa Jingumae Bldg. 3F, 2-4-11 Jingumae, Shibuya-ku, Tokyo, 150-0001
www.blueplanet-works.com/

information