Astellas Pharma Inc.

When Astellas Pharma migrated their corporate website to the cloud using Amazon Web Services (AWS), the company needed to secure their new AWS environment. To prevent malicious intrusion and website defacement, IT managers deployed Trend Micro Deep Security™.

**Challenge**

- In order to strengthen their disaster recovery plan and maintain website stability, Astellas migrated to Amazon Web Services (AWS). The company searched for a security solution specifically built for AWS.
- Before migrating to AWS, the company had been renting servers from a provider, making it impossible to implement individual security countermeasures on separate servers. The only web security they had was a firewall at the gateway.

**Solution**

The company selected the Amazon Cloud from Amazon Web Services (AWS) as the new platform for its corporate website.

"Although we were anxious about migrating to the cloud, AWS guarantees quality of service with a service-level agreement (SLA) and can distribute servers in data centers in Japan and overseas," says Hiraki. "We selected it because it guaranteed a high degree of reliability and availability, and was also reasonable from a cost perspective."

There was also another goal: strengthened security.

Astellas Pharma conducts pharmaceutical research and development based on a corporate philosophy of "contributing toward improving the health of people around the world through the provision of innovative and reliable pharmaceutical products."

The 2011 earthquake in Japan forced Astellas to review and strengthen its business continuity plans, including the function and stability of its corporate website. Their website fulfilled several important roles. Not only did it provide information for patients and their families, medical personnel, and shareholders and investors, it also featured the a3 (a•cube) site for recruiting collaborators for clinical trials and research.

"Because of the major earthquake, we realized that we needed to use something that operated 24/7 without interruption," explains Shuichi Hiraki, associate manager of infrastructure and IS for Astellas. "Up until that point, we had prepared a backup server on a remote site for disaster recovery, just in case. This required a manual switchover, and the host server was decrepit, so we decided to reconstruct the system to achieve a safer, more reliable environment."

To achieve this goal, the company had a number of requirements:
1) Disaster recovery between two data centers;
2) Faster and more efficient recovery;
3) Carryover of application assets;
4) Improved service availability when the system is overloaded; and
5) Reduction of IT costs.

**Results**

- The company implemented Trend Micro Deep Security, which runs on Amazon Web Services and enables Astellas to elastically add security for new AWS instances.
- With a complete set of security capabilities, including integrity monitoring, virtual patching, and anti-malware, the company has succeeded in maintaining the high level of security essential for business in a cloud environment.

**Customer Profile**

Astellas Pharma Inc.
Location: Tokyo, Japan
Established: 1923
Capital: $1 B USD (approx.)
Number of Employees: 17,454
Description: Manufacturer, distributor, importer/exporter of medical supplies

**Implemented Products/Solutions**

Trend Micro Deep Security™
Case Study  Cloud Security

“Due to the operational policies of the rental server provider, our existing environment was centered on gateway security via a firewall. It was impossible to implement the anti-malware software that we wanted to use on individual servers such as web servers and database servers. Although the provider had anti-malware service, it did not meet our requirements,” Hiraki explained. The application of security patches also created problems. “There were cases of patches affecting the operation of our applications. We wanted to perform operational checks on the patches in advance, but it wasn’t possible,” said Hiraki.

Astellas decided to solve its security problems at the same time they were migrating to AWS. Moreover, the company aimed to implement more advanced security and decided to implement Trend Micro Deep Security™.

The migration to AWS and implementation of Deep Security was carried out by FUJISOFT Inc., a recognized partner of both AWS and Trend Micro. The migration to AWS was carried out smoothly thanks to the extensive documentation from FUJISOFT Inc. They also provided full support for the implementation and configuration of Deep Security.

“In addition to the ability to implement anti-malware functions separately on each server, we highly value the comprehensive security functions that Deep Security has, such as IPS/IDS (intrusion detection and prevention), and virtual patching. At the time, we couldn’t find any other solution that guaranteed operation on AWS while also fulfilling our requirements. Furthermore, we had already implemented Trend Micro security solutions on our business PCs and servers, and were highly impressed with the quality of the products and Trend Micro’s courteous support. That degree of trust also led to the adoption,” said Hiraki.

Results

Currently, Astellas operates three virtual servers in AWS data centers in Japan as infrastructure for their corporate website. One server is used as a development and testing environment. The other two servers are deployed in data centers in different locations. Since the servers perform load balancing, there aren’t any concerns about service interruption - even if they are brought down by a disaster.

Data in the production environment is backed up in a data center located overseas. If an incident occurs in the domestic environment and the server becomes inoperable, service can continue because the data center is located overseas.

“The integrity monitoring function of Deep Security strengthened the system to monitor tampering, such as malicious system modification on our websites,” says Hiraki. “We plan to apply it to a number of programs, and web pages where personal information is entered.”

In the past, the service and labor costs from providers were extremely high for activities such as monitoring website defacement. Deep Security now allows Astellas to standardize the process and to monitor website defacement activities. In addition, the security log inspection function that detects failed login attempts is effective in preventing security attacks on passwords.

There are also high expectations for the virtual patching capability. With this function, an agent automatically detects recognized vulnerabilities and temporarily applies the necessary countermeasures for the vulnerability without waiting for an official patch. Once an official patch is verified and applied, the virtual patch is automatically removed. The virtual patching protects vulnerabilities until security patches are available and verified.

“We want use this function actively as a safety and security safeguard to protect our Operating System, Web Servers and Content Management System (CMS),” says Hiraki.

Using AWS and Deep Security, Astellas Pharma has successfully migrated its corporate website to the cloud. “It is difficult to keep up continuously with the new threats which are constantly emerging in the security field,” says Hiraki. “We have great hopes for the suggestions and services of Trend Micro, not to mention their friendly provision of information.


Amazon Web Services

- Domestic Data Center A
- Domestic Data Center B
- Overseas Data Center

- Production Environment
- Test Environment
- Backup Environment

- Trend Micro Deep Security™
  - Antivirus
  - Vulnerability countermeasures (IPS/IPS)
  - Web application protection
  - FireWall
  - Tamper monitoring
  - Security log monitoring

Contacts:

©2015 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro ball logo, Trend Micro Deep Security and Deep Security are trademarks or registered trademarks of Trend Micro, Incorporated. Amazon Web Services, the “Powered by Amazon Web Services” logo and other AWS Marks used in related materials are trademarks of Amazon.com, Inc., and/or its affiliates. This and other products/ company names may be service marks, trademarks or registered trademarks of their owners.

Information contained in this document is accurate as of June 2015 and subject to change without notice.

Trend Micro Incorporated
www.trendmicro.com

BR CASE-013