# Hikone City

ıllıllı
**CISCO**™

## Enhancing security measures and optimizing operations through " Network as a Sensor"



### Products and Services

- Cisco Network as a Sensor solution
- Cisco Advanced Malware Protection (AMP)

### Challenges

- Increased visibility to security on devices that are accessing the network and to integrate internal networks
- More robust measures against external threats and malware infections
- Gain network-wide visibility
- Optimization and cost control of security operations

### Solutions

- Cisco Network as a Sensor solution provides continuous monitoring of devices, applications and users throughout distributed networks quickly, and effectively responds to security breaches activity
- Cisco AMP analyzes files at point of entry to catch known and unknown malware, enabling faster time to detection and automatic protection

### Results and the Future

- Achieving both enhancement and optimization of security as a basis for administrative services

The city of Hikone, located in the northeastern part of Shiga prefecture boasts plenty of ruins, Shinto shrines and Buddhist temples, statues, paintings and other relics, including the ruins of Hikone castle. The city faces Lake Biwa, is surrounded by rich nature and serves as a high-traffic location near the Keihanshin, Chukyo and Hokuriku economic centers. The city administration works actively to promote tourism, and the activities of Hikonyan, the city's official mascot, have also become well-known.

> We would like to provide internal measures in the same way as the external measures. Cisco Solutions helps to analyze holistic network audit trails and achieve faster root-cause analysis, providing threat intelligence to accelerate incident response and optimize operations.
>
> —— Hikone City Information Policy Section
> Yasuhiro Yamamoto

Today, Hikone city is proceeding with a seismic retrofitting project for the city and government offices and is working to make the government service base more reliable. For ICT bases, we are integrating the internal networks (for government systems), which until now were constructed and operated as a separate units and external (Internet) access networks, in an effort to control labor and costs. We aim to enhance the communication environment used by city employees and improve and substantiate government services provided to city residents while facilitating speedy and accurate decisions as a municipality.

### Challenges

One of the issues with integration of the network was the improvement and consistency of security. In Hikone City, human involvement was not a main factor in operating the ICT infrastructure, and we are mainly focusing on reducing the workload of employees who are involved in such operations, as well as maintaining a certain level of security.
Yasuhiro Yamamoto of the Information Policy section said,
" With the recent national identification number and pension-related issues, municipalities must make security efforts. In our case, the number of people involved in operations is quite small, so we thought automation was needed to reduce the burden on management while maintaining a certain level of security.
We are reviewing our internal communication environment, but in the meantime, the number of terminals used by employees increased drastically from 180 units to 1,000 units, making the need for automation apparent. Integrating the network meant granting external access to multiple terminals, increasing the opportunity for threats.

Hikone City
Information Policy Section
Yasuhiro Yamamoto



Hikone City
Information Policy Section
Tatsuya Furukawa



Hikone City
Information Policy Section
Kimi Ueda

So, in order to prevent the spread of damage in case something does occur, we wanted to be able to stop communication automatically and isolate the terminal. Countermeasures for malware infections were also extremely important." A number of companies bid for Hikone City's system, but it was Cisco's "Network as a Sensor solution" and Cisco Advanced Malware Protection (AMP) that were selected. Mr. Yamamoto explains that the proposed content was superior and most suitable for the required conditions.

"It automatically monitors the behavior of the L3 network controlled by the switch, so if there is an employee accessing something that is not normally accessed, an alarm will go off automatically and that information will be retrieved. Log management is important in security operations, but oftentimes there isn't enough manpower, therefore a mechanism that monitors automatically and can respond to an extent is required, even if the log is not analyzed. It was a major concern what measures should be taken internally, in addition to external threats, but the Cisco proposal was clear on these points and we felt we could operate the system.

At first we were unsure of how far things could be automated and what types of products were available, but Cisco provides a total solution, which sealed the deal."

Kimi Ueda from the Information Policy section added to this statement.

"When everything is provided by one company, there is concern of vendor lock-in. However, there is comfort in the large number of development partners we have who are knowledgeable in Cisco products. Also, when multiple vendor products are combined, many problems occur, actually increasing the dependency on the specified development partners, making it difficult to entrust operations to other departments. We considered these points when making the final decision."

## We would like to increase network security and achieve effective operations, which will be the infrastructure, to provide better government services.

### Solutions

### Turning the entire network into a security sensor

Cisco's "Network as a Sensor" solution makes it possible to see threats on the network by combining real-time monitoring and alerts using Cisco StealthWatch and detailed traffic information generated with Cisco Catalyst series switch and Cisco IOS Flexible NetFlow. In Hikone City, Cisco Identity Services Engine (ISE), which performs access authentication and policy control, is also combined into the structure to further enhance security.

Tatsuya Furukawa from the Information Policy section said the following.

"In the future, when the city government gathers to consider what types of government services are needed to provide to all residents, it is extremely important to solidify a foundation based on security. There are a lot of questions concerning security measures, especially regarding the new national identification numbers, and there is a large difference in how these issues are handled between municipalities. Even as Hikone city boasts advanced efforts, I believe that the introduction of Cisco Solutions for this project has great significance. If you only look at the cost of security, it has increased compared to past figures, but the ICT infrastructure has reduced costs overall and maintains a position of full security coverage while minimizing cost and labor in other departments also."

2016 marks the 10th birthday of the official mascot, "Hikonyan"



### Anti-malware measures using Cisco AMP, industry-leading threat detection

Cisco AMP is an anti-malware product that detects and blocks malware, performs continuous analysis and issues alerts. Cisco synchronizes with the world's largest security infrastructure on a cloud system, providing comprehensive Malware protection throughout the entire cycle, before, during and after attacks, protecting the network and terminals from standard attacks, unknown threats and zero-day attacks. The detection rate was assessed to be the best the world by a third-party organization's study.

## Network as a Sensor (behavior detection)
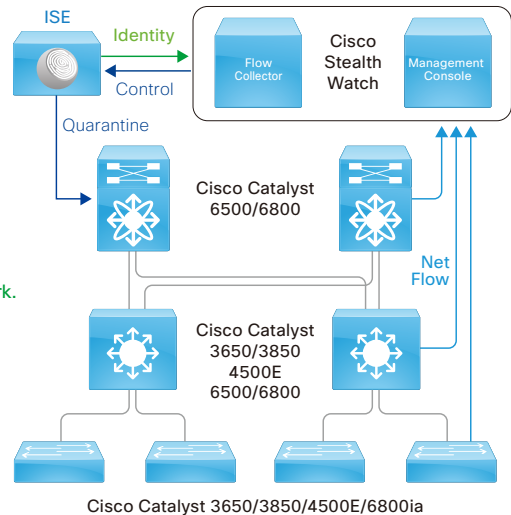## Network as a Sensor
Cisco IOS Flexible NetFlow/Cisco StealthWatch

- Deeper forensic investigations with audit histories of network activity
- Monitor anomalous behavior and security breach activities
- Reduce risk by understanding how, when, where, and why users and devices connect to the network.
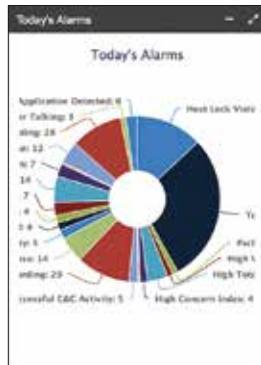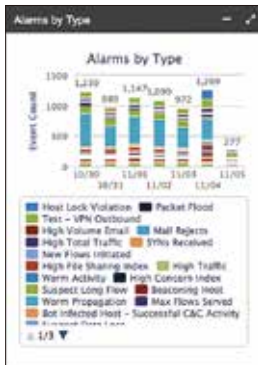
**Point**

- Flexible NetFlow enables optimization of the network infrastructure, reduced operation costs, and improved capacity planning and security incident detection with increased flexibility and scalability
- Ability to focus and monitor specific network behavior, and to monitor a wider range of packet information, producing new information about network behavior
- Flexible NetFlow enables the tracking of information within a NetFlow database or Flow Monitor
- No additional installation required for terminal and server software

ISE — Identity — Cisco Stealth Watch — Flow Collector — Management Console

Control

Quarantine

Cisco Catalyst 6500/6800

Cisco Catalyst 3650/3850 4500E 6500/6800

Net Flow

Cisco Catalyst 3650/3850/4500E/6800ia

## Management console dedicated to network sensor
## Cisco StealthWatch

Automatic identification of type of threat, communication path and target device from the traffic behavior information collected with the Cisco switch or router. Use time sequence to confirm what is occurring on which devices
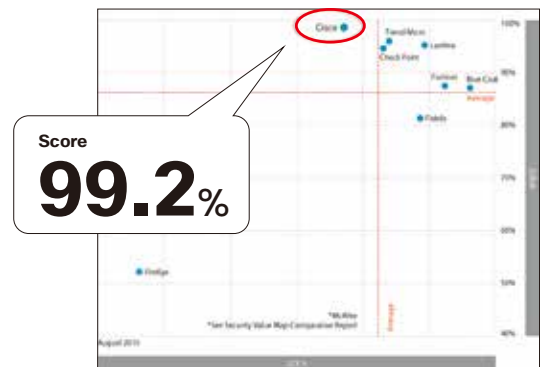
## Achieved the highest score in the NSS Labs Breach Detection Test
## Cisco AMP

Achieved the highest security effectiveness score in the NSS Labs Breach Detection System (BDS) Test.

Invasion detection system security value map

**Score**
**99.2%**

## Results and the Future

Construction of Hikone City's new network infrastructure is in progress and the first phase is expected to be completed by July 2016. After that, the goal is to complete the infrastructure in 2017 in line with the seismic retrofitting project. We will continue to improve government services, creating a town that is easy to live in and advancement of public welfare under the new ICT infrastructure.

### Other details and information

For more details on Cisco Network as a Sensor solution, please see
http://www.cisco.com/web/JP/solution/security/enterprise-network-security/net-sensor.html.
For details on Cisco AMP refer to www.cisco.com/jp/go/amp.

# Hikone City

**Hikone City Office**

| | |
|---|---|
| Address | 4-2 Motomachi, Hikone-shi, Shiga-ken |
| Scale | No. of Employees: 1,503 (as of April 2015) |
| | Population: 112,728 (55,676 male and 57,052 female) |
| | Households: 46,249 |
| | (As of July 2016) |
| URL | http://www.city.hikone.shiga.jp/ |

The Hikone City system was established on February 11, 1937, and thereafter developed as the main city on Lake Biwa's northeast side. This city, bordering Lake Biwa on one side and the Suzuka mountain range on the other, started as the town of a Hikone domain castle made up of 350,000 stones during the Edo Period. It now has a very historical and cultural atmosphere with reminders of the past dating from the middle ages to recent times, including many valuable historical items.