Case Study

Online Gaming Company Improves Network Visibility and Control

EXECUTIVE SUMMARY

Customer Name: Wargaming
Industry: Online gaming
Location: Global
Number of Employees: More than 4,000

Business Challenges

- Needed to protect intellectual property and maintain a competitive advantage
- Needed to secure a large, distributed global network
- Lacked centralized visibility across the environment

Network Solution

- Network visibility for advanced threat detection
- Identity and device data for added security context
- Improved access control and policy enforcement

Business Results

- Dramatically improved incident investigations
- Increased security team efficiency by saving time on incident analysis
- Enhanced network performance by quickly remediating slowdowns

Wargaming deploys Cisco Security for faster threat detection

Business Challenge

Wargaming is an award-winning online game developer and publisher across PC, console, and mobile. Founded in 1998, the company has shipped more than 15 titles and attracted over 150 million users. Wargaming employs over 4,000 people in 16 offices across North America, Europe, Asia, and Australia.

As an international organization, Wargaming has a large, widely distributed network. To secure its highly valuable intellectual property, the company needed a better way to visualize all of the traffic and users on its network. It also needed a better means of detecting potential threats, and when an incident did occur, it needed a way to quickly investigate and pinpoint the source.

Network Solution

First, Wargaming deployed the Cisco® Identity Services Engine (ISE) to obtain user and device data from across its global network. Cisco ISE helped Wargaming dramatically improve its security policy management and access control.

Next, the company wanted to further expand its network visibility by collecting and analyzing Cisco IOS® NetFlow. Its previous NetFlow analysis solution was not delivering enough data. Wargaming turned to the Cisco Stealthwatch® system to protect both its production network and the support network for its employees. Stealthwatch now collects and analyzes NetFlow data from Wargaming's existing Cisco routers and switches to dramatically expand visibility and security in the core of the company's network.

During its trial of Stealthwatch, Wargaming was able to detect two critical incidents with the technology. First, Stealthwatch discovered that someone from Wargaming's office supply vendor was scanning all of the company's http ports. Port scanning is often a sign of network reconnaissance, which is a primary step in many cyber attacks.

"Our integrated security solution gives us greater visibility and control over our network. It facilitates faster, more thorough forensic investigations."

Vasily Yanov
IP Network Team Lead, Wargaming

For More Information

Find out more about Cisco Stealthwatch and ISE at http://www.cisco.com/go/stealthwatch and http://www.cisco.com/go/ise.

Product List

Security

- Cisco Stealthwatch Flow Collector Series
- Cisco Stealthwatch Management Console
- Cisco Identity Services Engine (ISE)

Secondly, another person was discovered trying to access a database server and run a query that could destroy Wargaming's data. These are the types of anomalous behaviors that Stealthwatch is designed to detect. By identifying these potential threats early on in the attack, Stealthwatch can help prevent damaging data breaches before they occur.

Integrated Deployment

Today, Wargaming relies on an integrated global deployment of Cisco ISE and Stealthwatch to:

- Quickly detect potential threats across its network
- Identify the users and devices responsible
- Manage and enforce security policies
- Conduct faster, more thorough forensic investigations

Identity and device data from Cisco ISE is sent directly to the Stealthwatch Management Console. This way administrators can obtain a unified view of all network activities and assets through a single interface.

The ability to integrate various security technologies through one standard Cisco platform is critical to Wargaming's security success. Together, these technologies help Wargaming turn its existing Cisco network into an always-on security sensor. As a result, Wargaming can fill in gaps in its protection and reduce enterprise risk.

Business Results

With centralized network visibility, Wargaming has dramatically improved its incident investigations. Previously, if someone tried to obtain unauthorized access to its production data center, evidence of the incident would be erased from the system within a few days.

With Stealthwatch, Wargaming can retain months of NetFlow data. This way the security team can go back and uncover valuable details, such as who was involved in an incident, using which device, and at what time. This makes it much easier for Wargaming to continuously protect its valuable intellectual property and maintain a competitive advantage.

Wargaming's security team is also saving time with Stealthwatch. Now, using the system's automated, in-depth reports, the company can obtain a thorough picture of what happened during an incident within just 30 minutes.

Additionally, Stealthwatch is helping to improve Wargaming's network performance. It helps the IT team investigate traffic slowdowns and quickly reduce unnecessary use of bandwidth.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.

C36-738202-00 11/16