Cisco Builds an Email Security Solution for an Industry-Leading Manufacturer

EXECUTIVE SUMMARY

KOMATSU AT A GLANCE

Headquarters: Tokyo, Japan

Business: Worldwide industrial equipment and vehicle manufacturer

2007 Revenue: $1.6 billion in consolidated net sales

Employees: 33,836 (corporate); 6,231 (independent)

THE CISCO IRONPORT ADVANTAGE

- Proactive and reactive threat prevention and management with powerful email security and security management appliances
- Uniquely configured for Komatsu and its satellite offices, the Cisco IronPort C350 Email Security Appliance delivers superior security and reliability
- An estimated 75 percent increase in the detection of spam within one week of deployment
- Seamless management and updating for low cost of ownership with reduced administrative burdens and downtime

Overview

Tokyo-based Komatsu, Ltd., is a leading, global manufacturer of construction and mining equipment, industrial machinery, and vehicles. The company has recently partnered with Cisco® to implement an aggressive, comprehensive solution to combat spam, viruses, and associated threats across its wide email network.

The Situation

In 2004, in an environment of heightened regulatory scrutiny related to the security of sensitive information entering or leaving organizations (including the Japanese version of the Sarbanes-Oxley Act), Komatsu initiated an aggressive assessment of its overall corporate email security and threat deterrence capabilities to help ensure that the organization was complying to the fullest.

The study revealed a deteriorating ability to protect against spam. In 2005, the company selected a security vendor to address this growing challenge. The vendor's solution, however, failed to deliver sufficient detection, protection, and accuracy. By the summer of 2007, the amount of spam entering Komatsu's domestic corporate groups had grown exponentially - from roughly 40,000 messages per day in 2005 to 200,000 messages a day. This resulted in a major increase in the number of fraudulent messages reaching end users.

The problem was compounded by viruses entering the network as attachments to spam messages or embedded as URLs in the body of messages. With its existing security system, the organization was unable to automatically delete new virus-pattern files in time to prevent their spread. This forced Komatsu to enter into a new agreement with its security vendor to receive heightened services, including vaccines, and 24-hour customer service and system support.

> "By implementing Cisco IronPort products, we have obtained great results and are extremely satisfied."
>
> **— Kenichi Tabata, Department Supervisor, Komatsu**

Technical Challenges

Ultimately, Komatsu realized these email-based threats demanded a more comprehensive solution, rather than ongoing efforts to merely treat symptoms as they arose. The company determined that it required a solution that provided a best-in-class threat detection rate and the ability to identify and combat viruses as they emerged.

“Information security for the rapidly increasing spam volumes [had] become a crucial challenge,” said Kenichi Tabata, Komatsu Department Supervisor. “We were not satisfied with [previous] products that had a low detection rate of spam. So we chose to evaluate a new solution implementation. We also wanted to be able to quarantine emails with suspicious attachments prior to providing definition files.”

The Cisco IronPort Advantage

After a thorough search, Komatsu chose Cisco as its new email security provider, capitalizing on the proven power of the Cisco IronPort® C350 Email Security Appliance to provide advanced threat protection, block spam, and deliver easy enforcement of corporate policies. Designed to meet the email security needs of medium-sized corporations with satellite offices, the Cisco IronPort C350 uses both a proactive and reactive approach to fighting spam. Cisco IronPort Reputation Filters deliver real-time threat assessment and identify suspicious senders. Cisco IronPort Anti-Spam technology deploys a powerful, unique scanning engine to examine the full context of each message in order to stop the widest range of threats before they reach users. Additionally, the Cisco IronPort Spam Quarantine gives end users a safe holding area for spam messages that easily integrates with existing directory and mail systems.

One week after installing the Cisco IronPort C350 Email Security Appliance, Komatsu’s spam detection rate climbed from 200,000 per day to 346,000, quickly building end-user satisfaction and trust in the technology.

Cisco IronPort Virus Outbreak Filters are another powerful feature on these email security appliances. The filters provide Komatsu with a critical first layer of defense to accurately detect suspicious email attachments - often hours before traditional virus signatures are available - and automatically quarantine them. Fully integrated Sophos and McAfee antivirus technology delivers additional layers of defense to help ensure that problems are stopped before damage occurs.

The Cisco IronPort C350 also provides integrated compliance filters to guard against threats to regulatory compliance, advanced encryption capabilities to secure confidential data and comply with customers’ regulatory requirements, and the ability to quarantine messages that have been flagged by the content-scanning engine.

Advanced email authentication and enterprisewide management tools provide superior insight into threats as they arise. This reduces the administrative burden of handling problematic email, lowers costs by consolidating email operations and security onto a single platform, and increases productivity by serving as a shock absorber at the network gateway, protecting users from being bogged down by spam, viruses, and associated problems.

By implementing the Cisco IronPort M650 Security Management Appliance, Komatsu also enjoys flexible, comprehensive control at its gateway of all policy, reporting, and auditing information related to the Cisco IronPort Email Security Appliance. This centralized reporting capacity enables administrators to consolidate traffic data from multiple security appliances for fully integrated reporting.

“With Cisco, a substantial reduction in total cost of ownership and the new features to battle viruses and spam have been made a reality,” said Komatsu’s Kenichi Tabata. “By implementing Cisco IronPort products, we have obtained great results and are extremely satisfied.”

This document was originally published in 01/08, and is being republished with limited, non-substantive updates in 08/10.

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.**

Printed in USA C36-599562-00 10/10