CUSTOMER

Case Study

IRONPORT®

KOMATSU

IronPort Builds an Email Security Solution for an Industry-leading Manufacturer

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 IronPort® to implement an aggressive, comprehensive solution to combat spam, viruses and associated threats across its wide email network.

THE SITUATION

In 2004, amid a heightened regulatory environment 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 ensure its maximum compliance.

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) resulting in a major increase in the number of fraudulent messages passing through to end-users.

KOMATSU, LTD. 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 IRONPORT ADVANTAGE

- Proactive and reactive threat prevention and management with IronPort's powerful email security and security management appliances
- Uniquely configured for Komatsu and its satellite offices, the IronPort C350 delivers unrivaled 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

THE SITUATION (continued)

The problem was compounded by viruses entering the network as attachments to spam messages or embedded in messages' URLs. 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 receipt of vaccine offers, customer service and 24-hour system support.

TECHNICAL CHALLENGES

Ultimately, Komatsu realized these email-borne 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 IRONPORT ADVANTAGE

After a thorough search, Komatsu tapped IronPort as its new email security provider, capitalizing on the proven power of the 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 IronPort C350 utilizes a proactive and reactive approach to fighting spam. IronPort Reputation Filters deliver real-time threat assessment and identify suspicious senders, while IronPort Anti-Spam™ technology deploys a powerful, unique scanning engine to examine the full context of each message to stop the widest range of threats in their tracks. Additionally, the 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 IronPort C350, Komatsu's spam detection rate climbed from 200,000 per day to 346,000, quickly building end-user satisfaction and trust in the technology.

IronPort Virus Outbreak Filters™ are another powerful feature on IronPort's email security appliances. These 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 anti-virus technology delivers additional layers of defense to ensure problems are stopped before damage occurs.

THE IRONPORT ADVANTAGE (continued)

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

Advanced email authentication and enterprise-wide management tools provide unparalleled insight into threats as they arise. This reduces the administrative burden of handling problematic email, cuts costs by consolidating email operations and security onto a single platform, and increases productivity by serving as a shock absorber at the network gateway – ensuring that end-users aren't bogged down by spam, virus and associated problems.

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

"With IronPort, 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 IronPort products, we have obtained great results and are extremely satisfied."

IRONPORT 01/08 DOC RELEASE

IronPort Systems
950 Elm Avenue, San Bruno, California 94066
TEL 650.989.6500 FAX 650.989.6543
EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems, a Cisco business unit, is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase, the world's largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use—providing breakthrough performance and playing a mission-critical role in a company's network infrastructure.

IronPort is now part of Cisco.