

Yildiz Holding



Symantec Brightmail Gateway Significantly Reduces Number of False Positives and Spam Emails

Yildiz Holding, which includes Turkey's leading food brand Ulker, is benefiting from extensive protection for its emails, instant messages, and unconfigured data using Symantec™ Brightmail Gateway. This next generation security solution provides effective antispam and antivirus protection for incoming and outgoing emails, while also offering advanced technology for content filtering and data loss prevention. With a 99 percent spam filtering rate and an almost one-in-a-million possibility of false positive identification, Symantec Brightmail Gateway also possesses functionalities vital for companies like Yildiz Holding, such as automatic updates and global and local IP reputation analyzes. The solution also offers protection at quite a reasonable cost. It minimizes the potential risk related to incoming and outgoing emails while also reducing user-oriented management functions as much as possible thanks to its extensive reporting and administrative functions.

ORGANIZATION PROFILE

Yildiz Holding, which includes one of Turkey's leading food brands Ulker, demonstrates its leading and pioneering attitude to the whole world in the food group that it manages, its production and distribution strength, the variety of its products, and most importantly its vision.

INDUSTRY

Consumer Goods

SOLUTION

Messaging Security

“The Symantec Brightmail Gateway messaging security solution has many advantages in terms of both price and performance over its competitors. That is why we chose Symantec Brightmail Security and brought it to life with Tekbim's cooperation.”

Osman Veysel Erdag
Network Administrator
Yildiz Holding

High Frequency of False Positive Cases

Yildiz Holding is one of Turkey's leading groups, and includes Ulker, which began production in 1944 with a single type of biscuit. The company, which focuses on fast-moving consumer goods (FMCGs), operates in six main groups, with the emphasis on food. With 29,000 employees and a total of 42 domestic and international factories in Turkey, Romania, Ukraine, Algeria, Pakistan, Egypt, Saudi Arabia, Kazakhstan, Belgium, and America, Yildiz Holding offers a broad range of 2,700 different products, from biscuits to chocolate, and from ice cream to baby food. With sales of \$9.1 billion (2007) and the tax revenue that this generates, Yildiz Holding adds immense value to Turkey's economy.

The email traffic for most companies spirals year on year—and there's a corresponding rate of growth in email spam. This increase in both the volume and content of spam emails has led IT directors to search for a comprehensive security solution that inspires confidence by ensuring the prioritization of non-spam emails and the prevention of the loss of business caused by spam emails. “Our goal was not only to block spam emails from the network gateway but to reduce the number of false positive identifications as much as possible. Issues relating to loss of business, employee dissatisfaction, and their discomfort with the existing situation spurred us into action through the fear of reduced company productivity,” says Osman Veysel Erdag, Network Administrator, Yildiz Holding.

Comprehensive security solution prioritizes non-spam emails and increases productivity.

He continues, “With 29,000 employees and an extensive worldwide communications network, we were encountering a large number of spam and virus messages among our daily email traffic at Yildiz Holding. We communicate via email with many parts of the world, and these countries include many places that are on spam lists. This is why the existence and frequency of spam and emails containing viruses really constituted a serious problem for us. As well as all this, non-spam emails that were consigned to the spam folder presented major problems and were causing a loss of business. Due to this kind of false positive identification, we were losing sales and clients.”

Owing to these difficulties, the firm tested a number of solutions relating to messaging security. Owing to the false positive identification that they experienced during these tests, the team wanted to test Symantec Brightmail Gateway, which was considered by Yildiz to have a well-respected position in the marketplace. “The Symantec messaging solution had considerable advantages over its competitors, in terms of both performance and price; we had heard of the reputation of this Symantec product many times. This is why we selected Symantec Brightmail Gateway as a messaging security solution and brought it to life with Tekbim’s cooperation,” he says.

Compatible With a Heterogeneous Infrastructure

“Yildiz Holding’s technological infrastructure is located in three main data centers—two large ones and one smaller one. While the data center in Istanbul actively uses Symantec Brightmail Gateway, the data center in Ankara is a business continuity center, and here Brightmail is waiting passively on VMware.”

At these centers, which are built on an open systems architecture, VMWare virtualization is used extensively, and the virtual servers are structured on blade hardware. This infrastructure is supported by a Storage Area Network (SAN). The creation of a heterogeneous structure is envisioned, and servers and storage

“The solution, which also provides extensive protection against malware threats, has played an active role in the management of potential risks related to data loss, administrative activities within the company and regulatory conformance policies – and thus in the prevention of damage to the company’s reputation.”

Osman Veysel Erdag
Network Administrator
Yildiz Holding

SOLUTION AT A GLANCE

Business Drivers

- Increase work productivity
- Enable uninterrupted business
- Reduce the risk of business loss

Technology Challenges

- Provide extensive protection for messaging infrastructure
- Reduce the rate of spam emails and false positive identification to a minimum
- Increase service quality
- Reduce administrative costs

Solution

Symantec™ Brightmail Gateway messaging security solution offering comprehensive protection for unconfigured data,

Symantec Products

- Symantec™ Brightmail Gateway

Technology Environment

- Servers: HP®, IBM® physical servers, as well as virtual environments
- Operating systems: Microsoft® Windows®, Linux

Business Value and Technical Benefits

- Enabled effective and easy-to-use messaging security system
- Increased user productivity
- Introduced effective prevention of potential risks
- Reduced administrative expenses to a minimum
- Supported regulatory compliance policies

products from vendors such as HP, IBM, and EMC are used. A communications infrastructure based predominately on Windows and Linux has been installed—and a significant portion of the systems critical for operations are deployed in this environment.

Increase in Service Quality and Reduction in Administrative Costs

“With the removal of the disorder created by multiple consoles, fragmented policies, and ineffective reporting and logging activities, the solution reduced administrative expenses to a minimum.”

Osman Veysel Erdag
Network Administrator
Yildiz Holding

Osman Veysel Erdag comments, “I would first like to say that the installation of the solution is extremely simple and that its performance has been very successful. With respect to our own expectations, there was a significant reduction in false positives and spam emails. Not only did this mean that our work units gained more time and their productivity increased, it also meant an end to the complaints that reached our IT department. We were now protected against potential threats like the loss of work. The quality of service we provide increased enormously and our costs decreased.”

He adds that Symantec Brightmail Gateway effectively protects the company’s messaging infrastructure, and particularly emphasized that besides noticeably reducing spam emails and false positive identification—the solution has also contributed to employee productivity and potential work duration. “The solution, which also provides extensive protection against malware threats, has played an active role in the management of potential risks related to data loss, administrative activities within the company, and regulatory compliance policies, and thus the prevention of damage to the company’s reputation. With the removal of the disorder created by multiple consoles, fragmented policies, and ineffective reporting and logging activities, the solution reduced administrative expenses to a minimum.”