

# Case Study



Banking on Improved Email  
Performance and Security

## THE SITUATION

Dresdner Kleinwort Wasserstein (DrKW) is the investment division of Dresdner Bank AG and a member of the Allianz Group. Headquartered in London and Frankfurt, with an international network of offices in leading international financial centres such as New York and Tokyo, it employs approximately 6,000 people around the world. The impact of spam on storage requirements was becoming a real business challenge. Scaling storage to accommodate unwanted email was not the solution, DrKW needed to stop the problem before it hit the network and effected performance.



We chose IronPort because of the innovation in the technology. ”

### DRKW AT A GLANCE

Email users: 6,000

Challenge: 14% of incoming email is spam

### THE IRONPORT ADVANTAGE

- Increased email relay speed tenfold
- Eliminated 99 percent of spam
- Appliance with integrated anti-spam and anti-virus technology



### TECHNICAL CHALLENGES

Financial institutions are one of the main targets for unsolicited email. It is not unusual for between 40 and 50 percent of all email messages received by banks to be spam. Junk email is not just a drain on company email resources, it is also the channel through which many viruses, worms and other forms of malware are spread. This unrelenting rise in spam and unsolicited commercial email was having a detrimental affect on the IT infrastructure costs at DrKW.

DrKW had a very specific list of exacting requirements to be met. The extra performance and security needed to be built into their new solution to help reduce the existing number of infrastructure components. DrKW had two options; increase the number of legacy mail relays and existing mail transfer agents (to cater for the increase and expand of defences) or implement a new email security solution from the ground up.

The company's existing storage infrastructure was due for replacement, but the investment bank wanted to ensure there was no downtime or loss of performance. The requirement to get it right the first time made it particularly important to find the best solution, and DrKW piloted a number of products from different vendors.

DrKW's strict email security and compliance policies needed to be applied to every email. Consequently, the team was determined to find a solution that could apply these policies and improve email performance.

### THE IRONPORT SOLUTION

DrKW wanted an appliance with the ability to relay mail at least ten times faster than its existing solution. Anti-spam and anti-virus capabilities also needed to be built in to help simplify the infrastructure.

The company previously had anti-virus protection throughout the mail flow positioned at the perimeter, the email servers/file servers and at the desktop client. The bank wanted to maintain these three levels to provide the extra protection required in the financial services sector.

IronPort's appliance-based solution enabled the bank's messaging team to easily manage and set up the required policies. As with the rollout of any new solution, ease of implementation and support was always a key factor. DrKW deployed two IronPort C60™ appliances, one at each of its datacentres in London.



The IronPort C-Series email security appliance is easy to set up and manage.



### THE IRONPORT SOLUTION (CONTINUED)

As part of the financial institution's disaster recovery strategy the IronPort appliances supported an Active/Active datacenter topology. This involved using one IronPort C60 as the primary email centre and an identical appliance set up in an active (but idle) mode, ready to step in if needed.

Choosing IronPort® wasn't just down to the performance of the IronPort C-Series™, DrKW recognised the need to reduce the spam intake through new tactics and were eager to work with a company like IronPort that shares its vision about the importance of future defense mechanisms, such as Sender-ID and Sender Policy Framework (SPF) technologies.

The implementation was achieved within a month and commissioned into the live infrastructure within a couple of hours. The IronPort solution has already begun to deliver a return on investment. DrKW has been able to consolidate its corporate points of email presence (direct connections to an ISP) globally from three to one. This has helped the company to make substantial hardware and support cost savings.

The reduction in manpower time spent to support the boundary mail flow has meant that DrKW is able to deploy resources elsewhere in the company's infrastructure. This has helped to streamline and further reduce the administrative overhead of supporting other legacy systems. On average, 14 percent of DrKW's incoming mail is spam and the IronPort appliances are catching 99 percent of it on a daily basis.



#### IronPort Systems, Inc.

950 Elm Avenue, San Bruno, California 94066

TEL 650.989.6500 FAX 650.989.6543

EMAIL [info@ironport.com](mailto:info@ironport.com) WEB [www.ironport.com](http://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.

Copyright © 2000-2007 Cisco Systems, Inc. All rights reserved. IronPort, the IronPort logo and SenderBase are registered trademarks of Cisco Systems, Inc. All other trademarks are the property of Cisco Systems, Inc. or their respective owners. While every effort is made to ensure the information given is accurate, Cisco does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice. P/N 451-0116-1 10/07

IronPort is now  
part of Cisco.

