



# Nottingham University Hospitals NHS Trust

**Client:**

Nottingham University Hospitals  
NHS Trust (NUH)

**Web Site:**

www.nuh.nhs.uk

**Requirements:**

Email Filtering

**Filtering Solutions:**

M86 MailMarshal

“Unsolicited incoming offensive and pornographic emails were becoming a real problem within the organization. The previous system was labor intensive as it required constant monitoring to prevent false positives.”

Jonathan Phillips  
NUH ICT Systems Administrator

## Background

Nottingham University Hospitals NHS Trust (NUH) is one of the largest in the UK with an annual budget of more than £500 million.

It was formed on 1 April 2006 from the merger of two top-rated trusts: Queen's Medical Centre and Nottingham City Hospital. The aim of the merger was to develop a range of high-quality, sustainable patient services across the two campuses.

As a major teaching Trust, NUH enjoys close links with the city's universities and attracts and develops the highest caliber of staff. It continues to be the hospital of choice for patients, encourages investment and remains at the forefront of research.

NUH has one of the busiest emergency departments in the UK and has a total of 2,200 hospital beds across both campuses. To ensure the smooth running of the communications network the Trust has a team of 5 ICT administrators who maintain and protect the hospital's IT network and infrastructure, supporting 10,000 end users spread between the two hospital sites.

## The Spam Challenge

With a small ICT team supporting such a large number of end users, the challenge was to provide a robust external email filtering service which would filter out SPAM and inappropriate electronic content whilst still ensuring that medical related emails were not falsely blocked (known as “false-positives”). The ICT team also needed to ensure that any inbound attachments were free from viruses and malicious content.

Using an early version of Mimesweeper to scan and filter incoming emails, the ICT department at NUH was receiving on average 1 or 2 complaints a week about offensive and sometimes pornographic material getting through to employees' mailboxes.

“We also had a problem with the current software triggering false positives on a lot of medical related e-mails and it became a very manual process to check through the block list, looking for potentially legitimate e-mails which needed to be released,” reports Jonathan Phillips, NUH ICT Systems Administrator.

“Unsolicited incoming offensive and pornographic emails were becoming a real problem within the organization. The previous system was labor intensive as it required constant monitoring to prevent false positives.”

The ICT team began to look for a more sophisticated content filtering solution to replace the existing product. Phillips and colleague, Elizabeth Mackman, undertook a comprehensive review of anti-spam products including products from Clearswift, Surfcontrol and Trend Micro.

“M86 MailMarshal offered us really granular control over incoming and outbound emails to enable us to specify different policies and rule sets across the organization as required.”

Jonathan Phillips  
NUH ICT Systems Administrator

Evaluation was through on-site demonstrations and servers configured in a monitoring- only mode. After a suitable review period, NUH chose to deploy the M86 MailMarshal solution from integrated email and Internet content security provider M86.

Phillips reports that security software distributor Vigil Software was extremely helpful during the selection and implementation process. Vigil not only helped to install the software, but is also assisting Nottingham University Hospitals Trust with the planned upgrade of its infrastructure and the installation of the latest M86 MailMarshal upgrades.

## Implementation

Prior to roll out, M86 MailMarshal was run in monitoring only mode and new rules were turned on gradually to allow Phillips and his team to check the effect the rules had on email flow. If any issues were detected the rules were turned off and altered in order to not cause problems.

“M86 MailMarshal offered us really granular control over incoming and outbound emails to enable us to specify different policies and rule sets across the organization as required. It was really easy to reapply rules in a similar way to Outlook rule sets and we were able to tweak these to allow us to have the maximum filtering benefit, with the minimum number of false positives,” says Phillips.

M86 MailMarshal was rolled out at the Queen’s Medical Centre and Nottingham City Hospital campuses. At the time the two email systems operated independently from each other, handling two separate external email domains. It took just 2 days to complete the installation so M86 MailMarshal could go live as the email filtering system for the Trust.

## Key Benefits

With M86 MailMarshal, unlike the previous system, employees are now alerted when an email has been blocked due to a rule being triggered and the code they are emailed allows the ICT department to quickly locate and release the required email.

M86 MailMarshal also allows the ICT staff to create automated whitelists of acceptable email addresses, to both reduce the amount of spam and false positives. The NUH Trust keeps two whitelists, one for outgoing email and one for incoming emails. “M86 MailMarshal automatically updates its whitelist with email addresses mailed out from the Trust, because we can assume that these are legitimate. For incoming emails, we maintain a whitelist of NHS addresses which we check once a month to ensure that there are no updates or data entry errors,” Phillips explains.

As M86 MailMarshal rules are very similar to Microsoft Outlook rules, Phillips reports that creating and maintaining rule sets is very easy and does not require additional training. “It’s possible to create and implement new rules within minutes. Members of staff are now able to spend more time dealing with other work instead of spending on average 2 hours out of a working day looking at the blocked emails,” he says.

## Synopsis of key USPs and benefits delivered:

- NUH was receiving on average 1 or 2 complaints a week about offensive and sometimes pornographic material getting through to employees' mailboxes.
- Spam has been substantially reduced by blocking consistently 97 percent, but usually more than 99.5 per cent before it even reaches the NUH network.
- Malware contained within incoming attachments blocked 5 ICT administration staff supporting 10,000 end users spread across two hospital sites.
- Prior to M86 MailMarshal roll out, 2 members of the staff were spending up to 2 hours per day manually checking for false positives and releasing emails.
- Granularity of M86 MailMarshal rule sets and automated whitelisting of outgoing email addresses has freed up ICT staff to focus on their core roles.
- Up to 50 hours a week have been saved across the team.

## Future Plans

Phillips reports the ICT team is currently planning to refresh the hardware and reconfigure the M86 MailMarshal environment for the Trust. The plan is to merge the servers to bring the two separate systems into a true single email domain, allowing centralized management of the rule sets within the product and failover. The Trust will also use this upgrade as an opportunity to install updated software releases from M86.

Deployment of the M86 MailMarshal SPAM self release website is also planned, to enable employees to manage and maintain their own 'Blacklist' and 'Whitelist' for external email, while the ICT department will still maintain overall control of the system.

## ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry's leading Secure Web Gateway provider. The company's appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 24,000 customers and over 17 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advance threats, secure confidential information, and ensure regulatory compliance. The company is based in Orange, California with international headquarters in London and development centers in California, Israel, and New Zealand.

---

### TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit [www.m86security.com/downloads](http://www.m86security.com/downloads)



#### Corporate Headquarters

828 West Taft Avenue  
Orange, CA 92865  
United States  
Phone: +1 (714) 282-6111  
Fax: +1 (714) 282-6116

#### International Headquarters

Renaissance 2200  
Basing View, Basingstoke  
Hampshire RG21 4EQ  
United Kingdom  
Phone: +44 (0) 1256 848 080  
Fax: +44 (0) 1256 848 060

#### Asia-Pacific

Millennium Centre, Bldg C, Level 1  
600 Great South Road  
Ellerslie, Auckland, 1051  
New Zealand  
Phone: +64 (0) 9 984 5700  
Fax: +64 (0) 9 984 5720

Version 03.30.10