

The University of Nottingham Selects M86 to Secure Its Network from Web Threats

Client:

University of Nottingham

Website:

www.nottingham.ac.uk

Requirements:

Web Filtering and Reporting

Filtering Solutions:

M86 Secure Web Gateway

“As a global academic provider, Nottingham is always looking to implement best-of-breed enterprise solutions.”

Paul Kennedy
Security & Compliance Group Leader
Information Services

BACKGROUND

With origins dating back to 1881 and a Royal Charter granted in 1948, The University of Nottingham is a leading research university located in the East Midlands region of England. It has more than 36,000 registered students, including 7,500 international students from more than 145 countries. The university ranks in the top 10 of the best universities in the UK, the top 25 in Europe, and the top 70 worldwide, according to independent league tables.

In 1999, it opened an overseas campus in Malaysia and recently launched The University of Nottingham Ningbo in China. Alumni include the author DH Lawrence as well as Professor Sir Clive Granger, winner of the Nobel Prize for Economic Science in 2003. The university also has its own Nobel Prize winner, Professor Sir Peter Mansfield, who won the Nobel Prize for Medicine for his work in the application of magnetic resonance imaging (MRI).

Information Services, responsible for running the University network and core IT systems, was looking for a solution that would secure infrastructure and operations from external threats across its various campus locations.

The Internet has become a critical resource for a wide range of teaching and research activity for staff and students but remains liable to Web-borne attacks. Additionally, as a global academic enterprise with income of over £380 million, the university needed to secure its critical business systems and protect the online activities of its administrative staff. Protection against malicious code, spyware and crimeware was a top priority.

BUSINESS CHALLENGE AND REQUIREMENTS

In addition to protecting a campus network with 12,000 university-owned computers used for teaching, research and administration, Nottingham has a separate network for undergraduates in university accommodation which connects 8,000 student-owned PCs to campus resources and the Internet. The University needed to secure these computers and protect the privacy of students' personal information.

“Increases in Web-borne attacks mean that traditional signature-based anti-virus software alone is not enough. It cannot give us the protection we need against new and evolving malware threats. Students are often heavy users of social networking and other collaborative Web 2.0- enabled sites, which require more proactive threat detection and prevention techniques”, said Paul Kennedy, Security & Compliance Group Leader, Information Services.

“During the initial deployment we were able to identify a number of threats to the network that had previously been difficult to detect. Real-time code analysis gives us an additional tool in our armory for detecting and preventing crimeware attacks against university data and members’ personal information.”

Paul Kennedy
Security & Compliance Group Leader
Information Services

After an extensive evaluation, the university decided implement the M86 Secure Web Gateway with real-time code analysis technology to prevent Trojans and other malicious Web content from entering the network.

The separate campus and student networks require the university to define specific security policies for each. Students in university accommodation require access to services beyond the academic resources for their studies. These can be fully supported by a more flexible security policy on the student network than that deployed on the campus network.

Support for Internet access from 20,000 computers on the campus and student networks means the university has multiple gigabit connections to the East Midlands Metropolitan Area network (EMMAN) which in turn connects it to the UK Joint Academic Network (JANET). It therefore opted for an integrated gateway solution based around M86’s large enterprise SWG 7000 appliance. This provides a single point of management for real-time Web content scanning and anti-virus through multiple scanning blades.

M86 SECURE WEB GATEWAY SOLUTION

The University of Nottingham chose the M86 Secure Web Gateway solution after investigating a number of other leading gateway products and an extensive on-campus evaluation. M86’s proven and comprehensive solution features patented real-time code analysis technology to detect and block known and unknown malicious Web threats.

Deployed at the Internet gateway, the M86 Security solution has been integrated with the university’s existing Cisco Application Control Engine (ACE) load balancer to provide members with resilient Internet access via the multiple scanning blades within the M86 Security Bladecentre. Information Services security staff can manage activity via co-hosted policy server blades. These all-in-one appliances feature M86 real-time code analysis technology, Vulnerability Anti.dote™ and anti-spyware engines, as well as McAfee’s fully integrated anti-virus engine.

The M86 solution is deployed to provide coverage for the university’s five main campuses in Nottingham and nine satellite sites across the East Midlands. It secures campus data centers, staff desktops, student laptops, shared access computer rooms, an array of specialist laboratory equipment, and one of the most powerful, high-performance computer grids in the UK.

M86’s real-time code analysis technology is uniquely capable of analyzing Web content in real-time regardless of its source, breaking down the code and understanding its true intent without executing it on the end user’s machine. M86 delivers the highest rate of malicious code detection and prevention, allowing universities to safeguard their most valuable asset—their data.

By integrating several security engines in a single appliance, M86’s comprehensive solution facilitates rapid deployment, simplifies management, and reduces total cost of ownership. In addition, the appliance’s granular policy management lets the University of Nottingham enforce a flexible Web browsing environment by defining specific security policies for different parts of the network.

“M86’s real-time code analysis technology allows us to deal with a wider range of threats at the network perimeter, reducing incidents on the desktop and minimizing their impact on the university’s core academic and business activities.” said Kenney. Carl Burman, Sales Manager, Lucid IT Services, introduced Nottingham to the M86 Secure Web Gateway solution.

He commented, "Providing a solution to Nottingham University presented a number of unique challenges not normally found in the corporate environment. We worked closely with Paul Kennedy and M86 Security to provide a scalable solution which was capable of not just securing the campus networks but of providing comprehensive logging and reduced administrative overheads without affecting the end-user experience. We strongly believe the M86 solution meets all of these requirements and will continue to provide best-of-breed protection for years to come."

KEY BENEFITS TO THE UNIVERSITY OF NOTTINGHAM

- IT network secure from malicious and stealthy Web threats, such as crimeware and Trojans, that may bypass signature-based security methods
- Enhanced productivity through reduction of incidents and computer downtime
- Protection of business, teaching and research data as well as members' personal information
- Reduced administration effort and more efficient use of security resources
- Granular security policies for specific parts of the network
- Integrated security engines with single point of management and control

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 advanced 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



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 06/01/10