

CUSTOMER CASE STUDY

The National Trust



Customer Profile

The National Trust is an independently-funded organisation working to protect and preserve the U.K.'s coastline, countryside and historic properties throughout England, Wales and Northern Ireland.

With over 700 miles of coastline, 250,000 hectares of countryside, and moorland, and over 300 historic properties to maintain, including fine houses, castles, industrial monuments, mills, churches and pubs, the National Trust relies heavily on subscriptions from its 3.4 million members and donations made by the millions of people who visit its spectacular attractions each year.

However, the image of the National Trust as an organisation that simply looks after country gardens and historic homes, while visitors sit in its tranquil tea gardens is rather outdated. Its work stretches far beyond its traditional roots. The Trust makes important contributions to regeneration, education and the local environment through funding and sharing of expertise. Each year it invests over £160 million in the U.K.'s environmental infrastructure and has numerous long-term programmes in place aimed at educating people about the importance of the environment and of preserving the U.K.'s heritage for future generations. Protecting ancient buildings and coastline while preserving historical places of interest for future generations is a creative, not a static activity which involves having the foresight to embrace change and implement policies based on new ideas and thinking.

It was with this forward-looking attitude the National Trust's IT department approached the challenge of protecting its own assets, in this case its IT infrastructure. As can be seen with the structural designs of historic castles the Trust looks after, having a layered defence system offers the most effective perimeter protection against invaders while ensuring the integrity of assets held within. Similarly, an IT network which is only partially guarded against the latest evolving malware threats leaves itself exposed and vulnerable to attack, with the potential loss of sensitive and confidential data.

Over the past 12 months there has been a significant increase in sophisticated Web-based malware targeting large, enterprise-level corporate networks, searching and probing for weaknesses in IT defences.

The National Trust is no exception to such targeted attacks.

In order to protect its network from the growing number of Web threats, the National Trust evaluated a number of solutions, including on-premise hardware and software solutions. They opted instead for a managed security service to ensure the highest levels of security were maintained while allowing its IT team to focus its efforts on other business critical IT-related tasks.

The Challenge

The Web is an essential tool for National Trust and its regular, full-time staff of 5,000 relies heavily on having daily access to it in order to complete a range of business-critical tasks. These tasks include using applications that allow the management of historic properties,

About The National Trust



The National Trust was created for 'the benefit of the nation' and people are still at the heart of everything it does. The National Trust is committed to learning and creating opportunities for life-changing experiences, ensuring our historic houses, gardens, coastline and open countryside become spaces where visitors can experience inspiration, relaxation, enjoyment and enrichment for all. The National Trust is Europe's biggest conservation organisation, benefits from the support of over 3 million members and 40,000 volunteers and welcomes 500,000 school children every year.

Industry
Non-Profit

Solution
Web Malware Scanning and Web Filtering

Results

- Average of 165,000 malware blocks each month
- Average of 90,000 Web content blocks per month
- 'Zero' latency
- 24 x 7 real-time threat scanning
- Increased productivity and reduction in bandwidth consumption
- Centralized administration, management and reporting

For more case studies, visit
www.scansafe.com/resources

research, benchmarking tools, educational tools, publicising and promoting the Trust's work and allowing controlled access to staff for recreational Web surfing during permitted hours. The Web is also a key facilitator for the Trust when working on consultation documents, which involves the research and sharing of large amounts of information.

It was imperative that the Trust was able to control the costs of its network infrastructure while ensuring connectivity to its properties, each requiring secure Web access.

The Trust had a number of legacy IT security systems in place, which formed part of its layered defence network. Its firewall and VPN infrastructure helps provide it with a secure perimeter. The final area that required management and control was Web access, particularly as increasing numbers of mobile workers required remote access and VPN services.

"Different forms of malware have been around for some time now and we've always had effective measures in place to deal with this," said Dan Webster, Network Architect for the National Trust. "More recently, however, we've been very surprised at the volume of malware targeting enterprise networks. The rise in more sophisticated Web-based malware is certainly cause for concern. We're seeing a general rise in the number of Web threats probably being deployed by opportunists in a random manner. Twelve months ago there were few such threats coming in. In view of the threat landscape, the Trust started to search for a specialist IT security firm that dealt specifically with this kind of evolving threat."

The National Trust also needed a solution that could easily accommodate the nearly doubling of staff each summer in a number of locations.

"The National Trust is now Europe's largest voluntary organisation for nature conservation with more than 40,000 volunteers working for it," explains Steve Marsden, supplier manager, National Trust. "Each year the Trust's headcount more than doubles as part-time seasonal staff are employed throughout the country to cope with the increase in visitors to many of our sites. Staff numbers can grow up to 11,000 during the summer months. Many of these seasonal staff need access to the Web. We don't provide a blanket Web access policy for every employee so we needed a solution that would allow us to easily add new users and set user policies without requiring the costly and time consuming deployment of new hardware or software on multiple sites."

In addition, the National Trust also looked for a company that could deliver an impressive savings on total cost of ownership model (TCO) over a period of 3+ years and a service that, not only offered excellent value for money, but provided a range of useful features, such as a simple and effective reporting tool for its Web-based services.

The Solution

The National Trust considered several solutions, including products from SurfControl and Websense. However, on the advice from UKN Group, a Thames Valley-based specialist IT services firm which helps businesses improve the efficiency of their IT systems and services, the National Trust decided to try a 30-day risk free evaluation of ScanSafe's managed Web security services.

Following a successful evaluation, the National Trust implemented ScanSafe's Web Malware Scanning and Web Filtering.

Powered by ScanSafe's proactive technology - Outbreak Intelligence™, Web Malware Scanning offers protection from Web-borne viruses, spyware and adware. It blocks malware before it reaches the network, and identifies and blocks zero-hour threats — threats that appear before an anti-virus signature is available. This service also helps identify machines that are already infected with spyware and prevents them from 'calling home.'

Web Filtering provides control over how National Trust's employees use the Internet. It provides easy-to-use tools to create, enforce and monitor company Web usage policies. Using the most accurate categorisation databases, Web Filtering helps manage the organization's Internet traffic, protecting the network and staff from undesirable Web content.

The Result

National Trust opted for a managed security service solution as it required a certain level of expertise when dealing with Web-based malware. Unlike desktop software and appliances which require constant updating, the IT team now relies entirely on ScanSafe's experts to filter all Web traffic at source, ensuring it is free from malware.

On average, ScanSafe Web Malware Scanning blocks 165,000 instances of malware each month for National Trust. ScanSafe Web Filtering blocks on average around 90,000 instances of unwanted Web content each month, providing National Trust employees with a safe and productive Internet environment in which to carry out their valuable work.

"We are particularly impressed with ScanSafe's technical support team," Marsden says. "We tested the team's technical knowledge of its own product and also its general knowledge regarding the mechanical aspects of firewall configuration. The team's technical expertise is excellent and we rely heavily on this."

About ScanSafe SaaS Solutions

ScanSafe is the pioneer and largest global provider of SaaS Web Security, ensuring a safe and productive Internet environment for businesses. ScanSafe solutions keep malware off corporate networks and allow businesses to control and secure the use of the Web. As a SaaS solution, ScanSafe eliminates the burden of purchasing and maintaining infrastructure in-house, significantly lowering the total cost of ownership. Powered by its proactive, multilayered Outbreak Intelligence™ threat detection technology, ScanSafe processes billions of Web requests each month for thousands of enterprise customers.

In 2009, the company was awarded "Best Content Security" solution by SC Magazine Europe for the third consecutive year.

For more information, visit www.scansafe.com

ScanSafe US - 950 Elm Avenue, San Bruno, CA 94066 Tel: +1 650 989 7100 Fax: +1 650 989 6543 Email: ussales@scansafe.com

ScanSafe EMEA - Qube, 90 Whitfield St, London, W1T 4EZ Tel: +44 (0) 20 7034 9300 Fax: +44 (0) 20 7034 9301 Email: emeasales@scansafe.com



ScanSafe is now
part of Cisco.

