Network Security Case Study.

Upgrading to an Enterprise Antivirus solution.

How we improved our clients Network Security and increased their productivity by replacing their outdated Antivirus subscription with an Enterprise Endpoint Protection solution.
The challenge.

- Staff were complaining about continuous performance issues with their PCs
- A high percentage of support tickets that were logged by the previous IT incumbent were diagnosed as ‘malware or antivirus issues’
- The existing Antivirus solution was out of date and hadn’t been updated for over 8 months, putting their personal and client data at risk
- The client was using a mixture of Windows and Apple OSX-based servers to host their applications and client data

The solution.

- Replace the existing Antivirus subscription with Sophos Endpoint Protection. A highly advanced threat prevention solution that will provide the client with an enterprise level of protection on all devices across their network, including mobile devices.
- organised a number of group training sessions with the staff in order to develop and improve their information security awareness in the workplace.

The outcome.

- We completed the rollout of Sophos Endpoint protection suite in a day at both the London and New York offices with zero disruption to the client’s operations.
- The client now enjoys the highest level of enterprise protection against the latest network security threats.
- Automated scanning and updates are now in place for all devices.
- The staff are experiencing less antivirus/malware related issues on their PCs which has greatly increased productivity throughout the company.
- Less support tickets are being logged with our IT service desk team.
- Ongoing deployment and updates for both the London and New York office is maintained from a web-based management console.
Client overview.
Our client is a leading B2B software development company that was founded in 2009 by the present management. They provide bespoke web-based CRM applications to financial services organisations across the globe.

The company employs 57 staff members that operate from their head office in London and their satellite office located in New York.
The client recently switched to Our IT Department’s Fully Managed IT Support service because they were unhappy with the service provided by their existing incumbent. As with all new clients, our first task was to complete an IT Infrastructure audit and provide the client with a traffic light report containing our findings and recommendations for moving forward.

The staff were unhappy.
The client noticed that a large number of staff were complaining about the performance of their PCs or rather, the lack of it! This was particularly concerning because most of the hardware had solid specifications and was only 6 months old. In addition, they noticed that a high percentage of support tickets in the log were diagnosed as ‘malware or antivirus issues’ by the previous IT incumbent, yet the management team had not been notified of this persistent problem.

The existing Antivirus solution was outdated.
During the audit, we noticed the existing antivirus license subscription hadn’t been updated for over 8 months. This was putting their business at risk on many levels, including not just their own personal data but any client data that was being retained on their network during the application development process.

The client was still using the same antivirus solution they had been using for a long time and it wasn’t suitable for organisations with 50+ staff members. This level of protection was fine five years ago when they a smaller operation. However, it is no longer suitable because their staff base has since increased by 30 users.

Additionally.
The client was using a mixture of Windows and Apple OSX-based servers to host their applications and client data. The servers were also using the same outdated antivirus subscription.

Fortunately (and somewhat miraculously), the client had not yet fallen victim to a serious cyber-attack. However, the lack of threat detention was a ticking time bomb for the company that had to be deactivated before the inevitable happened.
“Malicious software poses an ever-increasing threat, not only due to the number of malware programs increasing, but also due to the nature of the threats. Infection vectors are changing from simple file based methods to distribution via the Internet. Malware is increasingly focusing on users, e.g. by deceiving them into visiting infected web pages, installing rogue/malicious software, cyber espionage, ransomware or opening emails with malicious attachments. The scope of protection offered by antivirus programs like signatures and heuristics must be extended by the inclusion of e.g. URL-blockers, content filtering, reputation systems, cloud based methodologies and user-friendly behavior-blockers.” – AV Comparatives, an independent antivirus application testing firm.

The solution.
Following a post IT Infrastructure audit meeting with the management team, Our IT Department proposed that the existing antivirus subscription be removed and replaced with Sophos Endpoint Protection. This is a highly advanced threat prevention solution that will provide the client with an enterprise level of protection on all devices across their network, including mobile devices.

Why Endpoint protection?
There are cheaper threat prevention solutions on the market that we could have recommended. However, Sophos is our preferred solution of choice for providing an enterprise level of protection required by an organisation that handles personally identifiable client data, albeit a small percentage of the data was 3rd party.

With GDPR on the horizon.
It was vitally important for our client to implement a solution that would contribute to their compliance before the GDPR regulations come into effect next year.
Additionally.
We were also conscious of the fact that the client was running cross platform operating systems in Windows and OSX respectively, in addition to Apple mobile devices that required an adequate level of protection. Sophos Endpoint protection runs on both operating systems together in a cross-platform environment.

Other reasons we choose Sophos Endpoint protection include:
Unlike other traditional antivirus solutions, Sophos Endpoint protection doesn’t rely on signatures to block malware. Instead, it correlates threat indicators that are used in just about every attack to block web and application exploits, dangerous URLs, potentially unwanted apps and malicious code. Endpoint protection incorporates:

- CryptoGuard anti-ransomware
- Anti-malware
- Web security
- Malicious traffic detection
- Deep system clean up
- Complete control.

The advanced version of Sophos Endpoint protection incorporates an advanced management console that allows us to deploy, manage and maintain the protection suite on every machine across the network in London and New York, including servers, workstations and mobile devices.

To summarise, Sophos Endpoint protection is by far one of the most advanced threat prevention solutions we’ve used, which is why we recommend it to our clients.

Staff awareness training.
During the original IT infrastructure audit, we spent some time with the staff discussing their IT and where they felt it could be improved. It became clear to us that the many of the staff lacked knowledge and awareness of the latest network security threats, a fact that is backed by the number of malware/virus related support tickets that were logged with the previous IT incumbent. Because of this, we organised a number of group training sessions with the staff in order to develop and improve their information security awareness in the workplace.

The client agreed with our proposal and we continued to proceed with the implementation of Endpoint Protection.
Our IT Department completed the rollout of Sophos Endpoint protection suite in a day at both the London and New York offices with zero disruption to the client’s operations. The project scope included the removal of the existing antivirus solution from all machines and the implementation of Sophos on 50 PCs, 10 laptops, 3 servers and a number of mobile devices. Inbound traffic is being filtered at both the gateway and the client’s mail server.

The entire roll out was completed remotely by our project management team.

- The client now enjoys the highest level of enterprise protection against the latest network security threats.
- Automated scanning and updates are now in place for all devices.
- The staff are experiencing less antivirus/malware related issues on their PCs which has greatly increased productivity throughout the company.
- Less support tickets are being logged with our IT service desk team.
- Ongoing deployment and updates for both the London and New York office is maintained from a web-based management console.

In addition.
We visited the London office and completed a series of group training sessions with all the staff members. We completed the staff training for the staff in the New York office via a number of video conferencing sessions.

**To Conclude...**
The client has now been using Sophos Endpoint Protection suite for 2 years. They are very happy with the performance of the solution and the fact that the number of viruses/malware related IT issues has been significantly reduced.
Let us improve your network security and productivity with Sophos Endpoint protection.

From consultation to deployment, we can implement and maintain the entire suite of award winning Sophos Network, end user and server protection solutions that will provide your business with the highest level of network security.

Contact us on 020 8501 7676 to find out how we’ll secure your business data and ensure you remain compliant.

**DID YOU KNOW?**

Our IT Department has been an official Sophos Partner for over ten years.
Where to find us.

Our London Office
22 Bevis Marks
London
EC3A 7JB

Located within a short walking Distance of the Gherkin.

Our East of England Office
6 Eaton Ct, Eaton Socon
Saint Neots
PE19 8ER

Located at Colmworth Business Park.

HOW TO CONTACT US.

Call us        020 8501 7676
Email us       info@ouritdept.co.uk

Tweet us       @ouritdepartment
Like us        /LondonITSupport