

ESET In Perfect Harmony With The London Symphony Orchestra

Switching antivirus vendors enabled the LSO to lower system resource utilisation and reduce costs with a product more suited to its needs.



CUSTOMER

Based in the Barbican in the City of London, the London Symphony Orchestra (LSO) is one of the best known orchestras in the world. In addition to a hectic concert schedule, the orchestra has a dazzling array of film credits to its name, undertakes pioneering work in digital music and encourages people of all ages to discover orchestral music through its education and community programmes.

To help reduce costs the LSO turns off its computers and related equipment when not in use. This means that vital tasks such as virus scanning must be carried out during office hours at a time when it is least disruptive, normally on Friday afternoons. However, when scanning started to impact heavily on performance of the network and the productivity of employees it was decided to look for a new supplier.

CHALLENGE

“Changing end-point security is not something you undertake lightly, it can be a lot of work and can cause a lot of disruption,” explains Quentin Bradley, ICT of the LSO. “We had been using the same end-point security for a number of years, but during this time we began to use less and less of the functionality included in the product. For instance when we switched to Windows 7 we decided to use the native firewall and as such no longer needed the 3rd party desktop firewall. Not only that, the product had become highly intrusive and our computers became essentially unusable during the Friday afternoon virus scans.”

With more than 120 servers, desktops and laptops to protect the LSO decided that a product that just delivered comprehensive antivirus and antimalware protection for their equipment would be the most cost efficient and appropriate solution.

SOLUTION

ESET Endpoint Antivirus delivers comprehensive antivirus and antispysware protection with a range of customisable options. Whilst the LSO still run their weekly scans on a Friday afternoon, ESET’s small footprint means the impact on performance is minimal. ESET Remote Administration enables the LSO to control all endpoints from a single console, ensuring that machines and servers are always fully protected.

“We chose ESET because of its small installation, relatively low demand on system resources and its high malware detection rate. It’s also worth noting that the technical support we have received from ESET has been absolutely great. One of the aspects we like about Endpoint Antivirus is that it can be configured to work exactly how we want it to, but sometimes this means a call into ESET just to clarify a technical point. Every question or issue has been dealt with by extremely knowledgeable and helpful people. They really know their product well.”



ENDPOINT ANTIVIRUS

FOR WINDOWS

ESET Endpoint Antivirus with award-winning ESET NOD32® technology delivers superior detection power for your business.

Its low system demands and virtualization capability keep your system humming.

Keep the security of offline devices under control, and customize scanning and update options as you see fit. Control it all effortlessly with our all-new, user-friendly remote administrator tool.

Antivirus and Antispyware	Eliminates all types of threats, including viruses, rootkits, worms and spyware. Optional cloud-powered scanning: Whitelisting of safe files based on file reputation database in the cloud for better detection and faster scanning. Only information about executable and archive files is sent to the cloud – such data are not personally attributable.
Virtualization Support	ESET Shared Local Cache stores metadata about already scanned files within the virtual environment so same files are not scanned again resulting in boosted scan speed. ESET module updates and virus signatures database are stored outside of the default location, thus these don't have to be downloaded every time after the virtual machine is reverted to default snapshot.
Host-Based Intrusion Prevention System (HIPS)	Enables you to define rules for system registry, processes, applications and files. Provides tampering protection and detects threats based on system behavior.
Exploit Blocker	Strengthens security of applications on users' systems, such as web browsers, PDF readers, email client or MS office components, which are commonly exploited. Monitors process behaviors and looks for suspicious activities typical of exploits. Strengthens protection against targeted attacks and previously unknown exploits, i.e. zero-day attacks.
Advanced Memory Scanner	Monitors the behavior of malicious processes and scans them once they decloak in the memory. This allows for effective infection prevention even from heavily obfuscated malware.
Cross-Platform Protection	ESET security solutions for Windows are capable of detecting Mac OS threats and vice-versa, delivering better protection in multi-platform environments.
Anti-Phishing	Protects end users from attempts by fake websites masquerading as trustworthy ones to acquire sensitive information such as usernames, passwords or banking and credit card details.
Device Control	Blocks unauthorized devices (CDs/DVDs and USBs) from your system. Enables you to create rules for user groups to comply with your company policies. Soft blocking notifies the end user his device is blocked and gives him the option to access the device, with activity logged.