Blenheim Palace Chooses a Stately Security Solution in ESET

Looking for a reliable and cost effective security solution that could meet the high demands of a popular tourist attraction, the team at Blenheim Palace turned to ESET for help. With proven protection ESET Endpoint Security was the perfect choice for their network.

CUSTOMER

Blenheim Palace is a UNESCO World Heritage Site visitor attraction based in Oxfordshire, attracting over 600,000 UK and international visitors every year. As well as attracting tourists all year round to the palace, park and gardens; Blenheim Palace also provides a venue for numerous special events, including seasonal children's activities, sporting events and iconic events such as The CLA Game Fair, Battle Proms Concert and Living Crafts for Christmas.

As a popular tourist attraction there is a heavy reliance on IT systems at the palace. According to Dave Horwell, IT Systems Manager at Blenheim Palace, "we rely on technology for admissions payment processing, 3rd parties rely on our systems to access their own payment processing and IT systems, visitor Wi-Fi, as well as all our own internal systems." In order to keep all areas of business running, they need to be able to rely on the stability of the network and the security software that protects it.

CHALLENGE

The previous security product used at Blenheim Palace offered the features required, but the price was a key issue which drove the team to look around at other solutions when the existing security solution came up for renewal. The challenge for the IT team was to find a more cost effective solution without compromising on security or putting the systems at risk.

Dave Horwell, IT Systems Manager, had previous positive experience of ESET products over a number of years and had used ESET several times in his home environment. He also looked to independent bodies such as Spiceworks for recommendations and reviews. It was essential that the security software company chosen could provide solutions to protect their key areas of IT usage including, finance, web, email, SharePoint server and SQL.

SOLUTION

After fully researching the products available on the market, they chose to approach ESET for a quote in the hope of getting the right features for the right deal. ESET Endpoint Security delivers unparalleled protection against viruses, spyware and other types of malware. Renowned for its low use of system resources, ESET Endpoint Security provides state of the art protection without increasing IT management overheads.

"ESET offered pretty much the same level of protection with a lower resource requirement for the client machines" says Dave Horwell, IT Systems Manager at Blenheim Palace. "The remote admin console is feature rich and has an addition of giving an overview of patch levels for client machines. All of this for half the price I would've paid had I stuck with the existing solution."

ENDPOINT SECURITY
FOR WINDOWS

ESET Endpoint Security delivers comprehensive IT security for your business via multiple layers of protection, including our field-proven ESET NOD32® detection technology, complete data access protection and fully adjustable scanning and update options.

Keep your system running at its best thanks to low system demands, virtualization support and optional cloud-powered scanning.

And oversee it all effortlessly with our completely redesigned, user-friendly remote administrator tool.

Chameleon Web Services
202 Dudley Road
Birmingham B63 3NR
0121 663 0456
admin@chameleonwebservices.co.uk
www.chameleonwebservices.co.uk

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 identical files are not scanned again, resulting in boosted scan speed. ESET module updates and virus signatures database are stored outside of the default location, so these don't have to be downloaded every time a 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 anti-tamper protection and detects threats based on system behavior.
Exploit Blocker	Strengthens security of applications such as web browsers, PDF readers, email clients 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.
Client Antispam	Effectively filters out spam and scans all incoming emails for malware. Native support for Microsoft Outlook (POP3, IMAP, MAPI).
Web Control	Limits website access by category, e.g. gaming, social networking, shopping and others. Enables you to create rules for user groups to comply with your company policies. Soft blocking – notifies the end user that the website is blocked giving him an option to access the website, with activity logged.
Anti-Phishing	Protects end users from attempts by fake websites to acquire sensitive information such as usernames, passwords or banking and credit card details.
Two-Way Firewall	Prevents unauthorized access to your company network. Provides anti-hacker protection and data exposure prevention. Lets you define trusted networks, making all other connections, such as to public Wi-Fi, in 'strict' mode by default. Troubleshooting wizard guides you through a set of questions, identifying problematic rules, or allowing you to create new ones.
Botnet Protection	Protects against infiltration by botnet malware – preventing spam and network attacks launched from the endpoint.
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 that his device is blocked and gives him the option to access the device, with activity logged.

ENJOY SAFER TECHNOLOGY™