ESET gives Powys the power to control their security

Powys County Council were looking to replace their existing Antivirus Software in schools as it wasn't providing the oversight and the security assurance that was required, but the prospect of removing the software from over 95 schools was daunting to say the least. Between COGO and ESET a smooth and bespoke transition was provided.

CUSTOMER

Powys County Council oversee over 95 schools, with more than 8000 seats. A number of those schools are very geographically remote, adding to the concern that Powys had over removing the antivirus software in favour of a more complete solution.

COGO offer Compliance and IT solutions working with Distology. ESET came to COGO's attention when Distology started offering ESET's solutions, following ESET's adoption of a two-tier channel model. As Eileen Buck, Director at COGO, explains, "working with Powys, I'm always aware of their finite resources but their intent to do every job to the highest quality. The support which ESET gave them throughout enabled that to happen."

CHALLENGE

Given the large number of schools and seats, with both geographically remote locations and a certain level of autonomy, the challenge was quickly removing the old AV and rolling out ESET across a number of separate domains.

Julie Davies, Cyber Security Officer at Powys County Council, explains, "We had concerns that a rip and replace method for remote schools might run into problems, combined with the fact that not all schools are connected to the same domain. We needed to ensure that all the schools were individually well catered for. Most schools do not have dedicated IT staff in place and teachers do not have time or resource to spend dealing with IT Issues. The deployment needed to have little interaction and ideally would be performed remotely as much as possible.

"Ongoing support has been invaluable. ESET's technical engineer Tom has given continuing support to an excellent standard. ESET were constantly touching base and provided us with a bespoke manual: they wanted to make sure that we were happy and went above and beyond."

SOLUTION

ESET Endpoint Protection Advanced, which incorporates ESET's File, Endpoint, Virtualization and Mobile Security, as well as Remote Management, was purchased for 8000 seats. "Support has been fantastic! Extremely user friendly and everything works perfectly. ESET discovered and rectified issues that we weren't aware were currently present, explains Julie.

Leon Griffiths, Senior Field Service Engineer at Powys County Council, adds that "previously we had no assurances that things were up to date: with ESET everything is easy to see and is updated as soon as it boots. We've had positive feedback from our end users: no slowdown on bandwidth, delegated management, ability to have their own policies per school, schools have their own independence to manage their domain taking some strain from us, while providing an overall view as well."

Eileen added, "COGO brings to their customers compliance and security solutions and ESET provide significant value in this marketplace. I was hugely impressed with the amount of technical expertise which was willingly brought to the party to make this implementation as smooth as possible."

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.

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.