Dorset Police Hi-Tech Crime Unit Relies on ESET Endpoint Antivirus

"Recreating data from a machine linked to crime would normally be asking for trouble, but we know that we can rely on ESET Endpoint Antivirus to identify the threats, whilst allowing us to decide what action to take."

DC Tristan Oliver , Dorset Hi-Tech Crime Unit

CUSTOMER

The Dorset Police Hi –Tech Crime Unit is instrumental in the investigation of computer related crime in the area and is responsible for gathering evidence for prosecution by examining and analysing data from machines connected to criminal activities.

CHALLENGE

"The trouble is when you're working in hi-tech crime you have two opposing sets of needs. One hand you require that your machines do not become infected, either from 'normal' sources or from something that may be lurking in the data of the machine being investigated. At the same time, if you are studying data from a suspect's computer and there is a virus, you may actually want to run it just to prove its exact intentions. Our forensic work can make it very challenging circumstances for antivirus products."

The Hi-Tech Crime Unit required an antivirus product that was light on system resources, operated in the background without being intrusive and yet would provide the flexibility to allow settings to be easily altered as required. In addition, the Hi-Tech Crime Unit required that it's secure network, which was not connected to the internet, could easily be updated with the latest virus signatures and engine updates.

SOLUTION

"We looked at several different products, but chose ESET Endpoint Antivirus as it met all our requirements and had an enviable reputation as the vendor with the most VB awards," continues Tristan Oliver. "Other products we looked at had nowhere near the same small footprint as Endpoint Antivirus and frequently tied up resources that we would prefer to be available for other processes. In addition, updating Endpoint Antivirus on our offline secure network is very easy, allowing us to keep these machines up-to-date with minimal administrative overhead."

"We've been using ESET Endpoint Antivirus since 2005 and ESET is still the vendor with the most VB100 awards and the one that as the smallest footprint, two of the key reasons we chose the product in the first place."

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.