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.”

Endpoint Antivirus can be configured to suit an organisation’s individual needs. Typically, companies require minimal user intervention and it is automatically set to delete or quarantine all suspicious files, reporting incidents to the administrator through the centralised management console.

“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.”

A high performing security solution built on an established track record in independent testing. Advanced technologies such as cloud-powered scanning and remote administration capability make it the right fit for any size company.

System Requirements:
Windows® 7, Vista, XP, 2000, NT 4.0 (SP6),
Windows Server 2000, 2003, 2008, 2008 R2

Processor Architecture:
Intel®/AMD® x86/x64

Antivirus and Antispyware

Eliminates all forms of threats, including viruses, rootkits, worms and spyware, keeping your network protected online and off. Optional cloud-powered scanning utilises our reputation database for increased scanning speed and minimal false positives.

NEW Host-based Intrusion Prevention System (HIPS)

Provides tampering protection and protects the system registry, processes, applications and files from unauthorised modification. You can customise the behaviour of the system down to every last detail and detect even unknown threats based on suspicious behaviour.

NEW Device Control

Lets you block unauthorised media and devices based on preset rules and parameters. Set access permissions (read/write, read, block) for individual media, devices, users and groups.

Auto-Scan of Removable Media

Automatically scans USBs, CDs, and DVDs for threats upon insertion to eliminate autorun and other removable risks. Choose from these scanning options: start automatically/notify (prompt user)/do not scan.

Cross-platform Protection

Exchange files and email attachments among Windows, Mac and Linux endpoints with confidence that malware targeting any of these platforms will be automatically detected and eliminated.

Prevent Macs turning into carriers of malware in the company network.

Low System Demands

Leaves more system resources for programs you use daily. Our software also runs smoothly on older hardware, saving your time and costs of having to upgrade your endpoints.

NEW Multiple Log Formats

Save logs in common formats - CSV, plain text, or Windows event log for immediate analysis or harvesting. Take advantage of data being readable by 3rd party SIEM tools; RSA enVision is supported directly via a plug-in.

NEW Update Rollback

Revert virus signature and module updates to a known good state in case of encountering system incompatibilities. Opt to freeze updates temporarily or until manually changed.